# Reference Manual for the ADSL Modem Wireless Router DG834GSP

NETGEAR

**NETGEAR**, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10262-01
June 2007

© 2007 by NETGEAR, Inc. All rights reserved.

## Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

## Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

## European Union Statement of Compliance

Hereby, NETGEAR, Inc. declares that this modem router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

| | |
|---|---|
| Èesky [Czech] | NETGEAR, Inc. tímto prohlašuje, že tento 54 Mbps ADSL Modem Wireless Router Model DG834GSP je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES. |
| Dansk [Danish] | Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr 54 Mbps ADSL Modem Wireless Router Model DG834GSP overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. |
| Deutsch [German] | Hiermit erklärt NETGEAR, Inc., dass sich das Gerät 54 Mbps ADSL Modem Wireless Router Model DG834GSP in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet. |
| Eesti [Estonian] | Käesolevaga kinnitab NETGEAR, Inc. seadme 54 Mbps ADSL Modem Wireless Router Model DG834GSP vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. |
| English | Hereby, NETGEAR, Inc., declares that this 54 Mbps ADSL Modem Wireless Router Model DG834GSP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. |
| Español [Spanish] | Por medio de la presente NETGEAR, Inc. declara que el 54 Mbps ADSL Modem Wireless Router Model DG834GSP cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE. |
| Ελληνική [Greek] | ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR, Inc. ΔΗΛΩΝΕΙ ΟΤΙ 54 Mbps ADSL Modem Wireless Router Model DG834GSP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ. |
| Français [French] | Par la présente NETGEAR, Inc. déclare que l'appareil 54 Mbps ADSL Modem Wireless Router Model DG834GSP est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. |
| Italiano [Italian] | Con la presente NETGEAR, Inc. dichiara che questo 54 Mbps ADSL Modem Wireless Router Model DG834GSP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE. |
| Latviski [Latvian] | Ar šo NETGEAR, Inc. deklarç, ka 54 Mbps ADSL Modem Wireless Router Model DG834GSP atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem. |
| Lietuviø [Lithuanian] | Šiuo NETGEAR, Inc. deklaruoja, kad šis 54 Mbps ADSL Modem Wireless Router Model DG834GSP atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas. |

| | |
|---|---|
| Nederlands [Dutch] | Hierbij verklaart NETGEAR, Inc. dat het toestel 54 Mbps ADSL Modem Wireless Router Model DG834GSP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. |
| Malti [Maltese] | Hawnhekk, NETGEAR, Inc., jiddikjara li dan 54 Mbps ADSL Modem Wireless Router Model DG834GSP jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC. |
| Magyar [Hungarian] | Alulírott, NETGEAR, Inc. nyilatkozom, hogy a 54 Mbps ADSL Modem Wireless Router Model DG834GSP megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak. |
| Polski [Polish] | Niniejszym NETGEAR, Inc. oœwiadcza, ¿e 54 Mbps ADSL Modem Wireless Router Model DG834GSP jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC. |
| Português [Portuguese] | NETGEAR, Inc. declara que este 54 Mbps ADSL Modem Wireless Router Model DG834GSP está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE. |
| Slovensko [Slovenian] | NETGEAR, Inc. izjavlja, da je ta 54 Mbps ADSL Modem Wireless Router Model DG834GSP v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES. |
| Slovensky [Slovak] | NETGEAR, Inc. týmto vyhlasuje, že 54 Mbps ADSL Modem Wireless Router Model DG834GSP spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES. |
| Suomi [Finnish] | NETGEAR, Inc. vakuuttaa täten että 54 Mbps ADSL Modem Wireless Router Model DG834GSP tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
| Svenska [Swedish] | Härmed intygar NETGEAR, Inc. att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG. |

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the DG834GSP product package.

### Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das 54 Mbps ADSL Modem Wireless Router Model DG834GSP gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

### Certificate of the Manufacturer/Importer

It is hereby certified that the 54 Mbps ADSL Modem Wireless Router Model DG834GSP has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

### Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

### Customer Support

Refer to the Support Information Card that shipped with your 54 Mbps ADSL Modem Wireless Router Model DG834GSP.

### World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

## Product and Publication Details

| | |
|---|---|
| **Model Number:** | DG834GSP |
| **Publication Date:** | June 2007 |
| **Product Family:** | Modem Router |
| **Product Name:** | 54 Mbps ADSL Modem Wireless Router Model DG834GSP |
| **Home or Business Product:** | Home |
| **Language:** | English |
| **Publication Part Number:** | 202-10262-01 |
| **Publication Version Number:** | 1.0 |

# Contents


## Reference Manual for the ADSL Modem Wireless Router DG834GSP

**Chapter 1**
**About This Manual**

Audience, Scope, Conventions, and Formats ..... 1-1
How to Print this Manual ..... 1-2

**Chapter 2**
**Introduction**

About the Modem Router ..... 2-1
Key Features ..... 2-2
A Powerful, True Firewall ..... 2-2
802.11 Standards-based Wireless Networking ..... 2-3
Easy Installation and Management ..... 2-3
Protocol Support ..... 2-4
Virtual Private Networking (VPN) ..... 2-5
Auto Sensing and Auto Uplink™ LAN Ethernet Connections ..... 2-5
Content Filtering ..... 2-6
Wi-Fi Multimedia (WMM) Quality of Service (QoS) ..... 2-6
What's in the Box? ..... 2-6
The Router's Front Panel ..... 2-8
The Router's Rear Panel ..... 2-9

**Chapter 3**
**Configuring Your Internet Connection**

Connecting the Router to the Internet ..... 3-1
Manual Setup ..... 3-1
What You Need Before You Begin ..... 3-1
Understanding ADSL Microfilters ..... 3-2
Computers Set to DHCP ..... 3-3
Manual Setup Procedure ..... 3-4

Auto-Detecting Your Internet Connection Type ....3-10
Wizard-Detected PPPoE Login Account Setup ....3-11
Wizard-Detected PPPoA Login Account Setup ....3-11
Wizard-Detected Dynamic IP Account Setup ....3-12
Wizard-Detected IP Over ATM Account Setup ....3-12
Wizard-Detected Fixed IP (Static) Account Setup ....3-13
Testing Your Internet Connection ....3-14
Manually Configuring Your Internet Connection ....3-15
How to Perform Manual Configuration ....3-16
ADSL Settings ....3-20

**Chapter 4**
**Wireless Configuration**

Considerations for a Wireless Network ....4-1
Observe Performance, Placement, and Range Guidelines ....4-1
Implement Appropriate Wireless Security ....4-2
Understanding Wireless Settings ....4-4
How to Set Up and Test Basic Wireless Connectivity ....4-7
How to Restrict Wireless Access to Your Network ....4-8
How to Configure WPA-PSK/WPA2-PSK Security ....4-11
How to Configure WPA-802.1x/WPA2-802.1x Security ....4-12
Choosing WEP Authentication and Security Encryption Methods ....4-13
How to Configure WEP ....4-14

**Chapter 5**
**Protecting Your Network**

Protecting Access to Your 54 Mbps ADSL Modem Wireless Router Model DG834GSP 5-1
How to Change the Built-In Password ....5-1
Changing the Administrator Login Timeout ....5-2
Configuring Basic Firewall Services ....5-3
Blocking Keywords, Sites, and Services ....5-3
How to Block Keywords and Sites ....5-3
Firewall Rules ....5-5
Inbound Rules (Port Forwarding) ....5-7
Outbound Rules (Service Blocking) ....5-9
Order of Precedence for Rules ....5-11
Services ....5-11

How to Define Services ....5-12
Setting Times and Scheduling Firewall Services ....5-13
How to Set Your Time Zone ....5-13
How to Schedule Firewall Services ....5-14

**Chapter 6**
**Managing Your Network**

Backing Up, Restoring, or Erasing Your Settings ....6-1
How to Back Up the Configuration to a File ....6-1
How to Restore the Configuration from a File ....6-2
How to Erase the Configuration ....6-2
Upgrading the Modem Router's Firmware ....6-2
How to Upgrade the Modem Router Firmware ....6-3
Network Management Information ....6-4
Viewing Modem Router Status and Usage Statistics ....6-4
Viewing Attached Devices ....6-9
Viewing, Selecting, and Saving Logged Information ....6-9
Examples of Log Messages ....6-12
Enabling Security Event E-mail Notification ....6-13
Running Diagnostic Utilities and Rebooting the Modem Router ....6-15
Enabling Remote Management ....6-16
Configuring Remote Management ....6-16

**Chapter 7**
**Advanced Configuration**

Configuring Advanced Security ....7-1
Setting Up A Default DMZ Server ....7-2
Connect Automatically, as Required ....7-3
Enable PPPoE-Relay ....7-4
Disable Port Scan and DOS Protection ....7-4
Respond to Ping on Internet WAN Port ....7-4
MTU Size ....7-4
Configuring LAN IP Settings ....7-4
DHCP ....7-6
How to Configure LAN TCP/IP Settings ....7-8
Configuring Dynamic DNS ....7-9
How to Configure Dynamic DNS ....7-10

Using Static Routes ..... 7-11
Static Route Example ..... 7-11
How to Configure Static Routes ..... 7-12
Universal Plug and Play (UPnP) ..... 7-13

**Chapter 8**
**Virtual Private Networking**

Overview of VPN Configuration ..... 8-2
Client-to-Gateway VPN Tunnels ..... 8-2
Gateway-to-Gateway VPN Tunnels ..... 8-3
Planning a VPN ..... 8-4
VPN Tunnel Configuration ..... 8-6
How to Set Up a Client-to-Gateway VPN Configuration ..... 8-7
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834GSP ..... 8-7
Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC ..... 8-12
How to Set Up a Gateway-to-Gateway VPN Configuration ..... 8-21
VPN Tunnel Control ..... 8-29
Activating a VPN Tunnel ..... 8-29
Verifying the Status of a VPN Tunnel ..... 8-33
Deactivating a VPN Tunnel ..... 8-35
Deleting a VPN Tunnel ..... 8-37
How to Set Up VPN Tunnels in Special Circumstances ..... 8-38
Using Auto Policy to Configure VPN Tunnels ..... 8-38
Using Manual Policy to Configure VPN Tunnels ..... 8-48

**Chapter 9**
**Troubleshooting**

Basic Functioning ..... 9-1
Power LED Not On ..... 9-2
Test LED Never Turns On or Test LED Stays On ..... 9-2
LAN or Internet Port LEDs Not On ..... 9-2
Troubleshooting the Web Configuration Interface ..... 9-3
Troubleshooting the ISP Connection ..... 9-4
ADSL link ..... 9-4
Obtaining a WAN IP Address ..... 9-5
Troubleshooting PPPoE or PPPoA ..... 9-6
Troubleshooting Internet Browsing ..... 9-7

Troubleshooting a TCP/IP Network Using the Ping Utility ..... 9-7
Testing the LAN Path to Your Router ..... 9-7
Testing the Path from Your Computer to a Remote Device ..... 9-8
Restoring the Default Configuration and Password ..... 9-9
Using the Reset button ..... 9-9
Problems with Date and Time ..... 9-9

**Appendix A**
**Technical Specifications**

**Appendix B**
**NETGEAR VPN Configuration**

DG834GSP to FVL328 ..... B-1
Configuration Profile ..... B-1
Step-By-Step Configuration ..... B-2
DG834GSP with FQDN to FVL328 ..... B-6
Configuration Profile ..... B-6
Step-By-Step Configuration ..... B-8
Configuration Summary (Telecommuter Example) ..... B-14
Setting Up the Client-to-Gateway VPN Configuration (Telecommuter Example) ..... B-14
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office ..... B-15
Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office ..... B-18
Monitoring the VPN Tunnel (Telecommuter Example) ..... B-28
Viewing the PC Client's Connection Monitor and Log Viewer ..... B-28
Viewing the VPN Router's VPN Status and Log Information ..... B-29

**Appendix C**
**Related Documents**

# Chapter 1
# About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

## Audience, Scope, Conventions, and Formats

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the Netgear website.

This guide uses the following typographical conventions:

**Table 1-1.**

| | |
|---|---|
| *italics* | Emphasis, books, CDs, URL names |
| bold | User input |
| `fixed` | Screen text, file and server names, extensions, commands, IP addresses |

This guide uses the following formats to highlight special messages:

**Note:** This format is used to highlight information of importance or special interest.

**Tip:** This format is used to highlight a procedure that will save time or resources.

**Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment.

**Danger:** This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

This manual is written for the ADSL Modem Wireless Router according to these specifications:

**Table 1-2. Manual Scope**

| | |
|---|---|
| Product Version | 54 Mbps ADSL Modem Wireless Router Model DG834GSP |
| Manual Publication Date | June 2007 |

## How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View**.

  Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter**.

  Use the *PDF of This Chapter* link at the top left of any page.

  — Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

  — Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

— Click the print icon in the upper left of the window.

**Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**.

  Use the *Complete PDF Manual* link at the top left of any page.

  — Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

  — Click the print icon in the upper left of the window.

**Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

# Chapter 2
# Introduction

This chapter describes the features of the NETGEAR 54 Mbps ADSL Modem Wireless Router Model DG834GSP. The ADSL Modem Wireless Router is a combination of a built-in ADSL modem, modem router, 4-port switch, and firewall which enables your entire network to safely share an Internet connection that otherwise would be used by a single computer.

**Note:** If you are unfamiliar with networking and routing, refer to "Internet Networking and TCP/IP Addressing" in Appendix C to become more familiar with the terms and procedures used in this manual.

## About the Modem Router

The 54 Mbps ADSL Modem Wireless Router Model DG834GSP provides continuous, high-speed 10/100 Ethernet access between your Ethernet devices. With minimum setup, you can install and use the modem router within minutes.

The ADSL Modem Wireless Router provides multiple Web content filtering options, reporting, and instant alerts. Parents and network administrators can establish restricted access policies based on time of day, Web site addresses, and address keywords. They can also share high-speed ADSL Internet access for up to 253 personal computers. The included firewall and Network Address Translation (NAT) features protect you from hackers.

# Key Features

The ADSL Modem Wireless Router provides the following features:

- A built-in ADSL modem
- A powerful, true firewall
- 802.11g standards-based wireless networking
- Easy, Web-based setup for installation and management
- Extensive Internet protocol support
- Trustworthy VPN Communications over the Internet
- VPN Wizard for easy VPN configuration
- Auto Sensing and Auto Uplink™ LAN Ethernet connections
- Content filtering
- Wi-Fi Multimedia (WMM) QoS (Quality of Service) to prioritize voice and video traffic

These features are discussed below.

## A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the DG834GSP is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection
  Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents
  The DG834GSP will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the modem router to email the log to you at specified intervals. You can also configure the modem router to send immediate alert messages to your email address or email pager whenever a significant event occurs.

## 802.11 Standards-based Wireless Networking

The ADSL Modem Wireless Router includes an 802.11g-compliant wireless access point, providing continuous, high-speed 10/100 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11g Standards-based wireless networking at up to 54 Mbps
- Works with both 802.11g and 802.11b wireless devices
- 64-bit and 128-bit WEP encryption security
- WEP keys can be entered manually or generated by passphrase
- Support for Wi-Fi Protected Access Pre-Shared Key (WPA-PSK and WPA2-PSK) encryption and 802.1x authentication
- Wireless access can be restricted by MAC address

## Easy Installation and Management

You can install, configure, and operate the DG834GSP within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-based management
  Browser-based configuration allows you to easily configure your modem router from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- Smart Wizard
  The firmware in the modem router automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- Remote management
  The modem router allows you to log in to the Web management interface from a remote location via the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, or you can choose a nonstandard port number.
- Diagnostic functions
  The modem router incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the modem router. You can use these diagnostic functions directly from the DG834GSP when you are connected on the LAN or when you are connected over the Internet via the remote management function.

- Visual monitoring
  The modem router's front panel LEDs provide an easy way to monitor its status and activity.
- Flash erasable programmable read-only memory (EPROM) for firmware upgrades.

## Protocol Support

The DG834GSP supports Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). "Internet Networking and TCP/IP Addressing" in Appendix C provides further information on TCP/IP.

- The Ability to Enable or Disable IP Address Sharing by NAT
  The DG834GSP allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account. This feature can also be turned off completely while using the DG834GSP if you want to manage the IP address scheme yourself.
- Automatic Configuration of Attached PCs by DHCP
  The DG834GSP dynamically assigns network configuration information, including IP, modem router, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- DNS Proxy
  When DHCP is enabled and no DNS addresses are specified, the modem router provides its own address as a DNS server to the attached PCs. The modem router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- Classical IP (RFC 1577)
  Some Internet service providers, in Europe for example, use Classical IP in their ADSL services. In such cases, the modem router is able to use the Classical IP address from the ISP.
- PPP over Ethernet (PPPoE)
  PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an ADSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your computer.
- PPP over ATM (PPPoA)
  PPP over ATM is a protocol for connecting remote hosts to the Internet over an ADSL connection by simulating an ATM connection.

- Point-to-Point Tunneling Protocol (PPTP)
  Typically used as a protocol for virtual private networks. This protocol is used by some Russian ISPs for connecting remote hosts to the Internet over an ADSL connection.

| | |
|---|---|
| | **Note:** PPTP must be manually configured. At present, the SmartWizard cannot automatically detect a PPTP type of connecton with your ISP. |

- Dynamic DNS
  Dynamic DNS services allow remote users to find your network using a domain name when your IP address is not permanently assigned. The modem router contains a client that can connect to many popular Dynamic DNS services to register your dynamic IP address.
- Universal Plug and Play (UPnP)
  UPnP is a networking architecture that provides compatibility between networking technologies. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

## Virtual Private Networking (VPN)

The ADSL Modem Wireless Router provides a secure encrypted connection between your local area network (LAN) and remote networks or clients. It includes the following VPN features:

- Supports 5 VPN connections.
- Supports industry standard VPN protocols
  The ADSL Modem Wireless Router supports standard Manual or IKE keying methods, standard MD5 and SHA-1 authentication methods, and standard DES and 3DES encryption methods. It is compatible with many other VPN products.
- Supports 3DES encryption for maximum security.
- VPN Wizard based on VPNC recommended settings.

## Auto Sensing and Auto Uplink™ LAN Ethernet Connections

With its internal 4-port 10/100 switch, the DG834GSP can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The local LAN ports are autosensing and capable of full-duplex or half-duplex operation.

The modem router incorporates Auto Uplink™ technology. Each local Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a computer or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

## Content Filtering

With its content filtering feature, the DG834GSP prevents objectionable content from reaching your PCs. The modem router allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the modem router to log and report attempts to access objectionable Internet sites.

## Wi-Fi Multimedia (WMM) Quality of Service (QoS)

WMM is a QoS feature that provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must be WMM-enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best-effort category, which receives a lower priority than voice and video.

# What’s in the Box?

The product package should contain the following items:

- 54 Mbps ADSL Modem Wireless Router Model DG834GSP
- AC power adapter (varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Microfilters (quantity and type vary by region)
- *DG834GSP ADSL Modem Wireless Router Resource CD*, including this guide
- Two plastic feet that can be used to stand the ADSL Modem Wireless Router on end
- Warranty and Support Information cards

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

## The Router's Front Panel

The front panel shown below contains status LEDs.

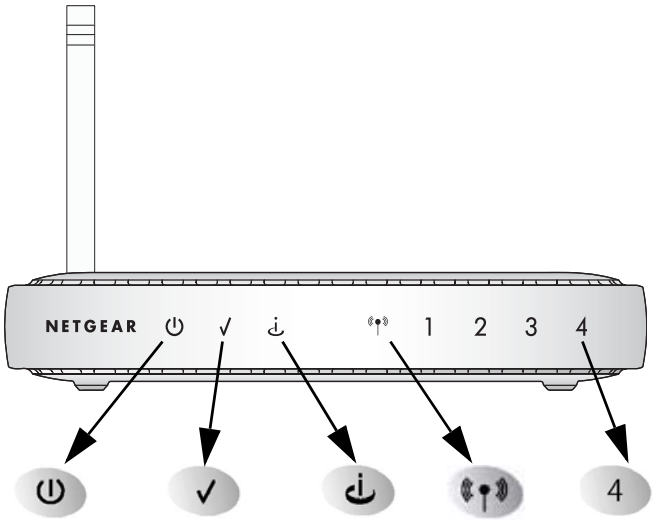



**Figure 2-1**

You can use the LEDs to verify various conditions. Table 2-1 describes each LED.

**Table 2-1. LED Descriptions**

| Label | Activity | Description |
|---|---|---|
| 1. Power | On<br>Off | Power is supplied to the router.<br>Power is not supplied to the router. |
| 2. Test | On<br>Off | The system is initializing.<br>The system is ready and running. |
| 3. Internet | On -- Green<br><br><br>Blink -- Green<br>On -- Amber<br><br>Blink -- Amber<br><br>Off | The Internet port is connected and an Internet session is in progress. If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green. If the session is dropped for any other reason, the LED color will change to amber.<br>Data is being transmitted or received by the Internet port.<br>The ADSL port is synchronized with your ISP's DSLAM but there is no Internet session.<br>The ADSL port is in the process of synchronizing with the your ISP's DSLAM.<br>No link is detected on the ADSL port. |

**Table 2-1. LED Descriptions (continued)**

| | | |
|---|---|---|
| 4. Wireless | On<br>Off | Indicates that the Wireless port is initialized.<br>The Wireless Access Point is turned off. |
| 5. LAN | On (Green)<br>Blink (Green)<br>On (Amber)<br>Blink (Amber)<br>Off | The Local port has detected a link with a 100 Mbps device.<br>Data is being transmitted or received at 100 Mbps.<br>The Local port has detected a link with a 10 Mbps device.<br>Data is being transmitted or received at 10 Mbps.<br>No link is detected on this port. |

## The Router's Rear Panel

The rear panel of the 54 Mbps ADSL Modem Wireless Router Model DG834GSP (Figure 2-2) contains port connections.

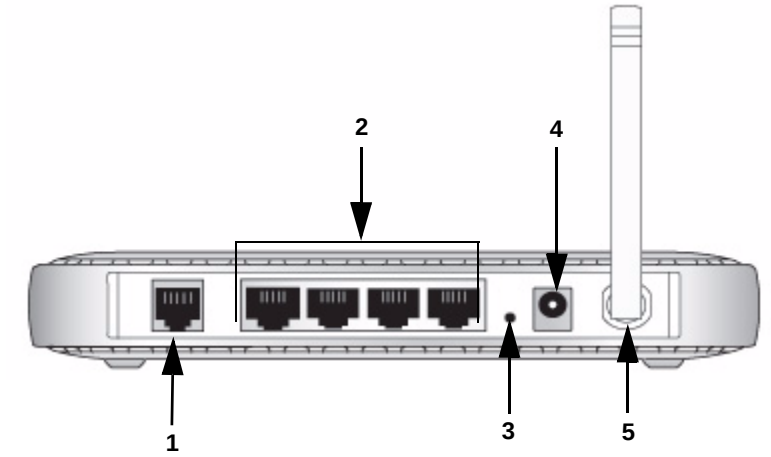



**Figure 2-2**

Viewed from left to right, the rear panel contains the following elements:

1. RJ-11 ADSL port for connecting the firewall to an ADSL line
2. Four Local Ethernet RJ-45 LAN ports for connecting the firewall to the local computers
3. Factory Default Reset push button
4. AC power adapter outlet
5. Wireless antenna

# Chapter 3
# Configuring Your Internet Connection

This chapter describes how to configure the wired internet connection of your 54 Mbps ADSL Modem Wireless Router Model DG834GSP.

## Connecting the Router to the Internet

To connect your ADSL Modem Wireless Router to the Internet, refer to the *ADSL Modem Wirelesss Router Setup Manual* on the *DG834GSP ADSL Modem Wireless Router Resource CD*

## Manual Setup

**Note:** The most reliable way to set up your modem router is by performing the setup from the CD, because it will be tailored to the configuration requirements of your ISP. You will only need to perform a setup from your router's configuration utility if you change your ISP or you are troubleshooting your connection.

Use the topics and procedures below to manually set up your modem router.

### What You Need Before You Begin

You need to prepare the following before you can set up your modem router:

- Active Internet service provided by an ADSL account.
- The Internet Service Provider (ISP) configuration information for your ADSL account.
  - ISP Login Name and Password
  - ISP Domain Name Server (DNS) Addresses
  - Fixed or Static IP Address
- ASDL microfilters as explained below.
- Your computers set to DHCP.

Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it.

### Internet Configuration Requirements

Depending on how your ISP set up your Internet account, you need one or more of these configuration parameters to connect your modem router to the Internet:

- Virtual Path Identifier (VPI)/Virtual Channel Indentifier (VCI) parameters
- Multiplexing Method
- Host and Domain Names

## Understanding ADSL Microfilters

ADSL technology uses the same wires as your telephone service. However, ADSL adds signals to the telephone lines which create noise in the telephone service. You must use ADSL microfilters to filter out these signals before they reach your telephone.

| | |
|---|---|
| | **Note:** If you purchased the modem router in a country where a microfilter is not included, you must acquire one. |

### ADSL Microfilter

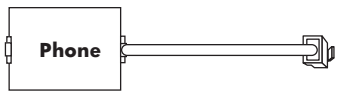



**Figure 3-1**

Each device such as a telephone, fax machine, answering machine, or caller ID display will require an ADSL microfilter.

| | |
|---|---|
| | **Warning:** Do not connect the modem router to the ADSL line through a microfilter unless the microfilter is a combination microfilter/splitter specifically designed for this purpose. Doing so will prevent block your connection to the Internet. If you have any doubts about this, connect the modem router directly to the ADSL line. |

**ADSL Microfilter with Built-In Splitter**

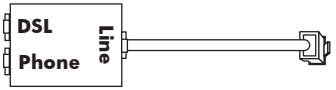



**Figure 3-2**

Use an ADSL microfilter with built-in splitter when there is a single wall outlet which must provide connectivity for both the modem router and telephone equipment.

## Computers Set to DHCP

For the initial connection to your modem router, your computer has to be set to automatically get its TCP/IP configuration from the modem router via DHCP. This is usually the case. The NETGEAR Smart Wizard CD automatically takes care of this requirement. For manual setup, refer to the documentation that came with your computer.

# Manual Setup Procedure

There are four steps to setting up your modem router:

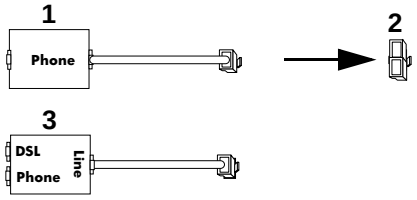
1. Install ADSL filters on the phone lines.
2. Connect the modem router to the ADSL line.
3. Log in to the modem router.
4. Connect to the Internet.

Follow the steps below to connect your modem router to your network. Before you begin, locate the ADSL configuration information from your Internet Service Provider (ISP).

**1.** Connect the ADSL filter.

> **Note:** If you purchased the DG834GSP in a country where an ADSL filter is not included, you must acquire one.

a. You need to install an ADSL filter for every telephone that uses the same phone line as your modem router. Select the filter that came with your modem router.




1. One-Line Filter: Use with a phone or fax machine.
2. Splitter: Use with a one-line filter to share an outlet with a phone and the modem router.
3. Two-Line Filter with Splitter: Use to share an outlet with a phone and the modem router.

**Figure 3-3**

b. **Two-Line Filter Example**. Insert the two-line filter into the phone outlet and connect the phone to the phone line connector (**A)**:

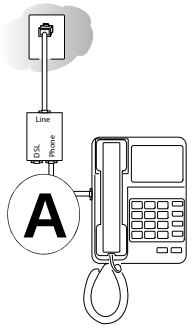



**Figure 3-4**

| | |
|---|---|
| | **Note:** To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter. |

**2.** Connect the modem router to the ADSL filter.

a. Using the included phone cable with RJ-11 jacks, connect the ADSL port (**B)** of the modem router to the ADSL port (**C)** of the two-line filter.

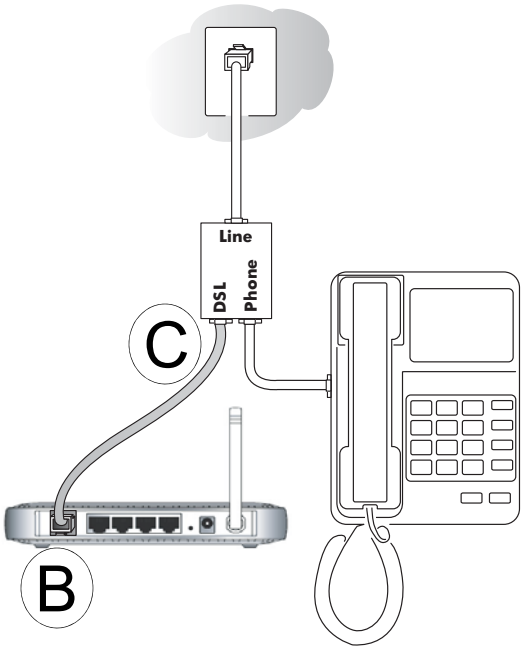



**Figure 3-5**

| | |
|---|---|
| | **Warning:** Improperly connecting a filter to your modem router will block your ADSL connection. |

b. Connect the Ethernet cable (**D)** from a modem router LAN port to the Ethernet adapter in your computer.

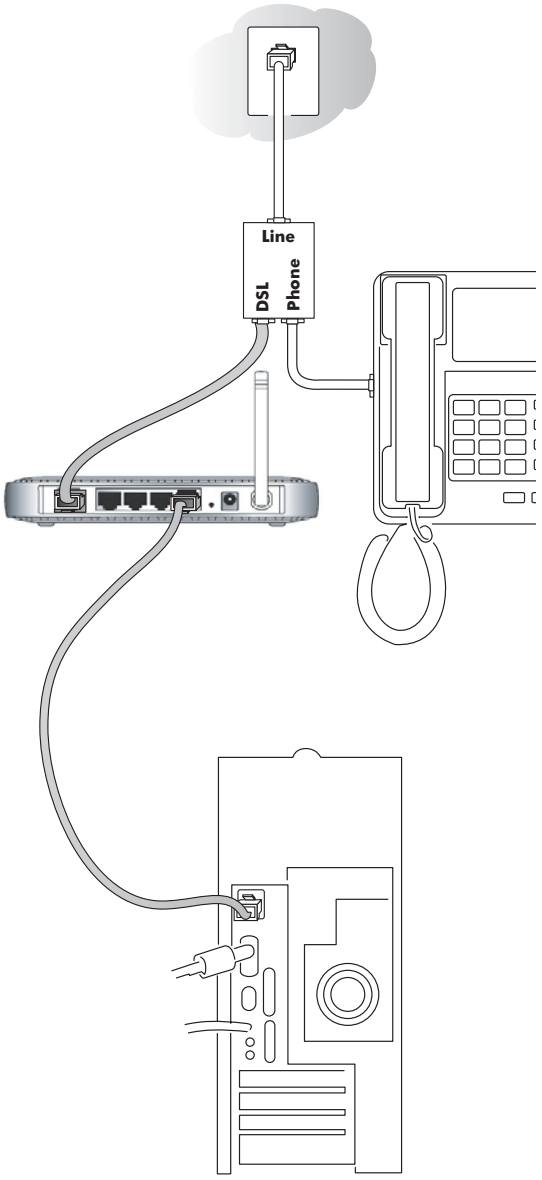



**Figure 3-6**

c. Connect the power adapter to the modem router and plug it in to a power outlet. Verify the following:

The power light is lit after turning on the modem router.

The test light comes on briefly, then goes off.

The wireless light is lit after turning on the modem router.

The ADSL light is amber, indicating you have a physical connection to the ADSL network.

d. Now, turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically. Verify the following:

The local LAN lights are lit for any connected computers.

**3.** Log in to the modem router.

**Note:** Your computer needs to be configured for DHCP. For instructions on configuring for DHCP, please see the documentation that came with your computer or "Preparing a Computer for Network Access" in Appendix C.

a. Type http://10.1.1.1 in the address field of a browser such as Internet Explorer or Netscape® Navigator.

This login window opens:

**Figure 3-7**

Enter **admin** for the user name and **password** for the password, both in lower case letters.

b. After logging in, you will see the menu below.

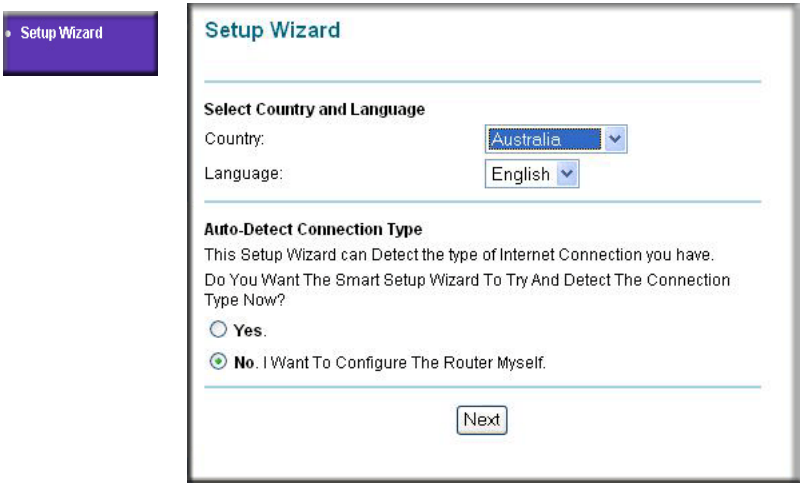

Setup Wizard
Setup Wizard
Select Country and Language
Country:
Australia
Language:
English
Auto-Detect Connection Type
This Setup Wizard can Detect the type of Internet Connection you have.
Do You Want The Smart Setup Wizard To Try And Detect The Connection Type Now?
Yes.
No. I Want To Configure The Router Myself.
Next

**Figure 3-8**

4. Connect to the Internet

   You are now ready to configure your modem router to connect to the Internet. There are two ways you can configure your modem router to connect to the Internet:

   a. Let the modem router Setup Wizard auto-detect the type of Internet connection you have and configure it. For more details, refer to "Auto-Detecting Your Internet Connection Type" on page 3-10

   b. Manually choose which type of Internet connection you have and configure it. For more details, refer to "Manually Configuring Your Internet Connection" on page 3-15

   In either case, use to the configuration parameters your ISP provided to assure that the configuration settings for your Internet connection are correct.

5. Test your Internet connection.

   From the bottom of the Setup menu, click Test. If the NETGEAR Web site does not appear within one minute, refer to Chapter 9, "Troubleshooting".

Your modem router is now configured to provide Internet access for your network. Your modem router automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as Dial-Up Networking or Enternet to connect, log in, or disconnect. These functions are performed automatically by the modem router as needed.

To access the Internet from any computer connected to your modem router, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the modem router's Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

## Auto-Detecting Your Internet Connection Type

The Web Configuration Manager built in to the modem router contains a Setup Wizard that can automatically determine your network connection type.

The procedures for filling in the configuration page for each type of connection follow below.

**Note:** At present, the SmartWizard cannot automatically detect a PPTP type of connecton with your ISP. If your ISP uses this type of protocol you must configure your connection manually (see "Manual Setup Procedure" on page 3-4).

## Wizard-Detected PPPoE Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over Ethernet (PPPoE), you will be directed to the PPPoE page shown:

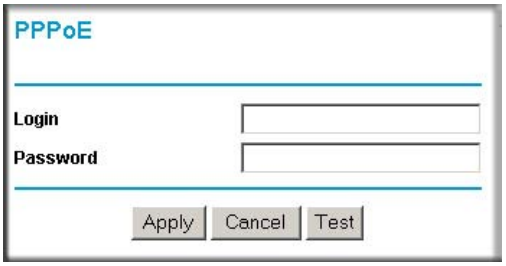



**Figure 3-9**

Enter the PPPoE login user name and password.

## Wizard-Detected PPPoA Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over ATM (PPPoA), you will be directed to the PPPoA page shown:

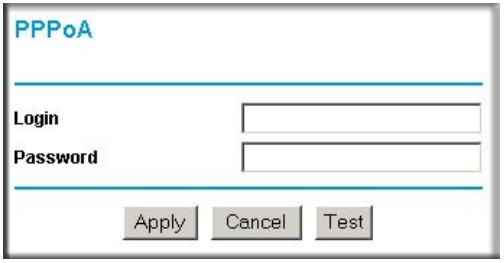



**Figure 3-10**

Enter your login user name and password. These fields are case sensitive.

## Wizard-Detected Dynamic IP Account Setup

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the page shown:

**Figure 3-11**

Click Apply to set Dynamic IP as the connection method.

## Wizard-Detected IP Over ATM Account Setup

If the Setup Wizard determines that your Internet service account uses IP over ATM Classical IP assignment (RFC1577), you will be directed to the page shown:

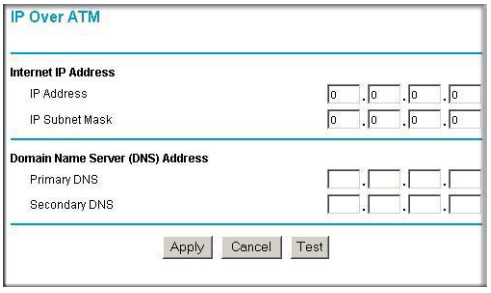



**Figure 3-12**

1. Enter your assigned IP Address and Subnet Mask. This information should have been provided to you by your ISP. You need the configuration parameters from your ISP.
2. Enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

DNS servers are required to perform the function of translating an Internet name such as *www.netgear.com* to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here.

3. Click Apply to save the settings.
4. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 9, "Troubleshooting".

## Wizard-Detected Fixed IP (Static) Account Setup

If the router determines that your Internet service account uses Fixed IP assignment, you will be directed to the page where you can enter the IP addresses.

1. If required, enter the Account Name and Domain Name from your ISP.
2. Choose "Use Static IP Address" or "Use IP Over ATM" (IPoA — RFC1483 Routed) according to the information from your ISP. If you choose IPoA, the router will be able to detect the gateway IP address but you still need to provide the router IP address.
3. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP's gateway modem router. This information should have been provided to you by your ISP. You need the configuration parameters from your ISP.
4. Enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

   DNS servers are required to perform the function of translating an Internet name such as *www.netgear.com* to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here.
5. Click Apply to save the settings.
6. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 9, "Troubleshooting".

# Testing Your Internet Connection

After completing the Internet connection configuration, your can test your Internet connection. Log in to the modem router, then, from the Basic Settings link in the Setup menu, click the Test button. If the NETGEAR Web site does not appear within one minute, refer to Chapter 9, "Troubleshooting".

Your modem router is now configured to provide Internet access for your network. Your modem router automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as Dial-Up Networking or Enternet to connect, log in, or disconnect. These functions are performed by the modem router as needed.

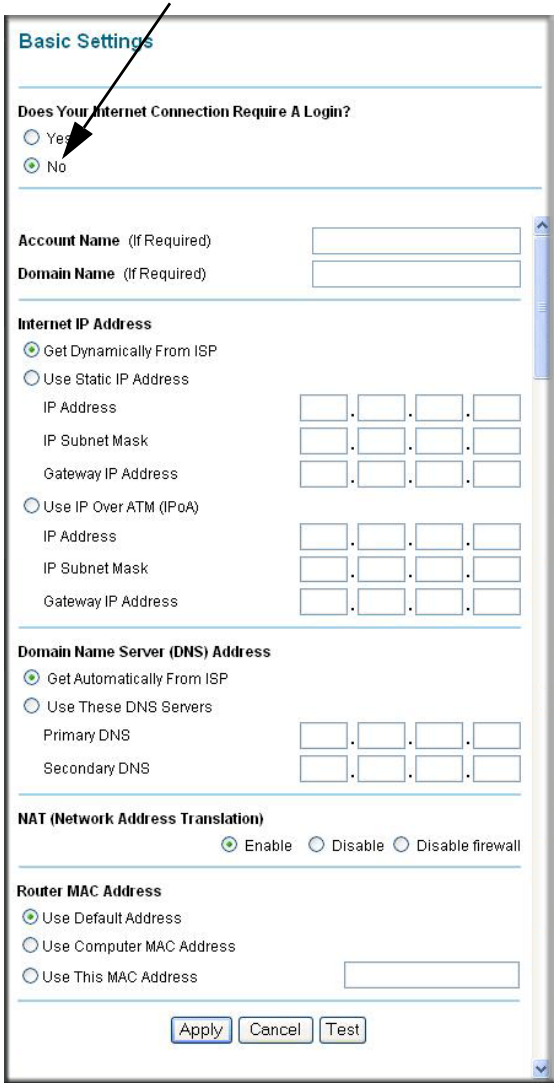
To access the Internet from any computer connected to your modem router, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the modem router's Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

The following chapters describe how to configure the Advanced features of your modem router, and how to troubleshoot problems that may occur.

# Manually Configuring Your Internet Connection

You can manually configure your modem router using the menu below, or you can allow the Setup Wizard to determine your configuration as described in the previous section.

**ISP *Does Not* Require Login**




**ISP *Does* Require Login**

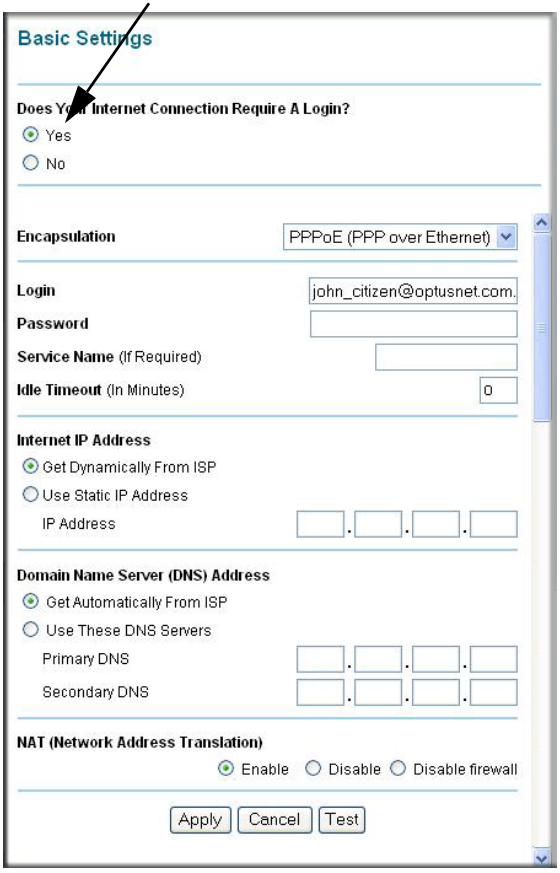



**Figure 3-13**

## How to Perform Manual Configuration

We recommend that you start the manual configuration from the Setup Wizard:

1. Select your country and language. Language choices are English, French, German, and Italian. After you change the language, the remaining setup screens change to the language of your choice.
2. Select No to manually configure your modem router connection.
3. Click **Next**.
4. Manually configure the modem router in the Basic Settings menu shown above.
5. Follow the instructions below according to the encapsulation method and whether your Internet connection requires a login. The following methods are available:
   - Internet Connection Requires Login and Uses PPPoE
   - Internet Connection Requires Login and Uses PPPoA
   - Internet Connection Does Not Require a Login
6. Usually the default ADSL Settings work fine for most ISPs and you can skip this step. If you have any problems with your connection, check the ADSL Settings. See "ADSL Settings" on page 3-20 for more details.

### Internet Connection Requires Login and Uses PPPoE

1. If your Internet connection *does* require login, select Yes and fill in the settings according to the instructions below.

**Note:** You will no longer need to launch the ISP's login program on your computer in order to access the Internet. When you start an Internet application, your modem router automatically logs you in.

2. Choose PPPoE for the encapsulation method.
3. Enter the login name (frequently the email address your ISP provided), password, and service name (if required).
4. If you want to change the login timeout, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of zero means never log out.
5. When a connection uses PPPoE, the IP address is normally assigned automatically. However, the DG834GSP allows this address to be set manually.

- Select “Get Dynamically from ISP” if your ISP assigns your IP address.
- Select “Use Static IP Address” if your ISP gave you a statically assigned address.

**6.** The DNS server is used to look up site addresses based on their names.

- Select “Get Automatically from ISP” if your ISP uses DHCP to assign your DNS servers. Your ISP will automatically assign this address.
- Select “Use These DNS Servers” if your ISP gave you one or two DNS addresses. Type the primary and secondary addresses.

**7.** You should only disable NAT if you are sure you do not require it. NAT automatically assigns private IP addresses (10.1.1.x) to LAN connected devices. When NAT is disabled, only standard routing is performed by this router.
Classical routing lets you directly manage the IP addresses the DG834GSP uses. Classical routing should be selected only by experienced users.

**Note:** Disabling NAT will reboot the router and reset all the DG834GSP configuration settings to the factory default. Disable NAT only if you plan to install the DG834GSP in a setting where you will be manually administering the IP address space on the LAN side of the router.

The “Disable Firewall” option disables the firewall in addition to disabling NAT. The “Disable” option leaves the firewall active. With the firewall disabled, the protections normally provided to your network will be disabled.

### Internet Connection Requires Login and Uses PPPoA

**1.** If your Internet connection *does* require login, select Yes and fill in the settings according to the instructions below.

**Note:** You will no longer need to launch the ISP’s login program on your computer in order to access the Internet. When you start an Internet application, your modem router automatically logs you in.

**2.** Choose PPPoA for the encapsulation method.

**3.** Enter the login name (frequently the email address your ISP provided), and password.

**4.** If you want to change the login timeout, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of zero means never log out.

5. When a connection uses PPPoA, the IP address is normally assigned automatically. However, the DG834GSP allows this address to be set manually.
   - Select “Get Dynamically from ISP” if your ISP assigns your IP address.
   - Select “Use Static IP Address” if your ISP gave you a statically assigned address.
6. The DNS server is used to look up site addresses based on their names.
   - Select “Get Automatically from ISP” if your ISP uses DHCP to assign your DNS servers. Your ISP will automatically assign this address.
   - Select “Use These DNS Servers” if your ISP gave you one or two DNS addresses. Type the primary and secondary addresses.You should only disable NAT if you are sure you do not require it.
7. NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices. When NAT is disabled, only standard routing is performed by this router.
   Classical routing lets you directly manage the IP addresses the DG834GSP uses. Classical routing should be selected only by experienced users.

**Note:** Disabling NAT will reboot the router and reset all the DG834GSP configuration settings to the factory default. Disable NAT only if you plan to install the DG834GSP in a setting where you will be manually administering the IP address space on the LAN side of the router.

The “Disable Firewall” option disables the firewall in addition to disabling NAT. The “Disable” option leaves the firewall active. With the firewall disabled, the protections normally provided to your network will be disabled.

### Internet Connection Requires Login and Uses PPTP

1. If your Internet connection *does* require login, select Yes and fill in the settings according to the instructions below.

**Note:** You will no longer need to launch the ISP’s login program on your computer in order to access the Internet. When you start an Internet application, your modem router automatically logs you in.

2. Choose PPTP Client for the encapsulation method.
3. Set the following items using the information assigned to you by your ISP:
   - Your local IP address and IP subnet mask
   - The server IP address for your ISP

- Your user name and password

### Internet Connection Does Not Require A Login

1. If your Internet connection does *not* require a login, select No and fill in the settings according to the instructions below.
2. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's mail or news servers.
3. Internet IP Address:
   - Select "Get Dynamically from ISP" if your ISP uses DHCP to assign your IP address. Your ISP will automatically assign these addresses.
   - Select "Use Static IP Address" if your ISP has assigned you a permanent, fixed (static) IP address. Enter the IP address that your ISP assigned. Also enter the IP Subnet Mask and the Gateway IP Address. The gateway is the ISP's modem router to which your modem router will connect.
   - Select "IP Over ATM (IPoA)" if your ISP uses Classical IP Addresses (RFC1577). Enter the IP address, IP Subnet Mask, and Gateway IP Addresses that your ISP assigned.
4. Domain Name Server (DNS) Address:
   - Select "Get Dynamically from ISP" if your ISP uses DHCP to assign your IP address. Your ISP will automatically assign this address.
   - If you know that your ISP does not automatically transmit DNS addresses to the modem router during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

   A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your modem router during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here.
5. You should only disable NAT if you are sure you do not require it. NAT automatically assigns private IP addresses (10.1.1.x) to LAN connected devices. When NAT is disabled, only standard routing is performed by this router.

   Classical routing lets you directly manage the IP addresses the DG834GSP uses. Classical routing should be selected only by experienced users.

| | |
|---|---|
| | **Note:** Disabling NAT will reboot the router and reset all the DG834GSP configuration settings to the factory default. Disable NAT only if you plan to install the DG834GSP in a setting where you will be manually administering the IP address space on the LAN side of the router. |

6. The “Disable Firewall” option disables the firewall in addition to disabling NAT. The “Disable” option leaves the firewall active. With the firewall disabled, the protections normally provided to your network will be disabled.

7. Modem Router MAC Address:
   This section determines the Ethernet MAC address that will be used by the modem router on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your modem router to masquerade as that computer by “cloning” its MAC address.

   To change the MAC address, select “Use this Computer’s MAC address”. The modem router will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. Alternatively, select “Use this MAC address” and enter it.

8. Click **Apply** to save your settings.

9. Click **Test** to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 9, “Troubleshooting”.

## ADSL Settings

The default settings of your 54 Mbps ADSL Modem Wireless Router Model DG834GSP will work fine for most ISPs. However, some ISPs use a specific Multiplexing Method and Virtual Circuit Number for the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI).

**Note:** The correct country must be selected from the Setup Wizard’s first page for the default ADSL Settings to work.

If your ISP provided you with a specific Multiplexing Method or VPI/VCI number, then fill in the following:

1. Select the ADSL Settings link from the main menu.

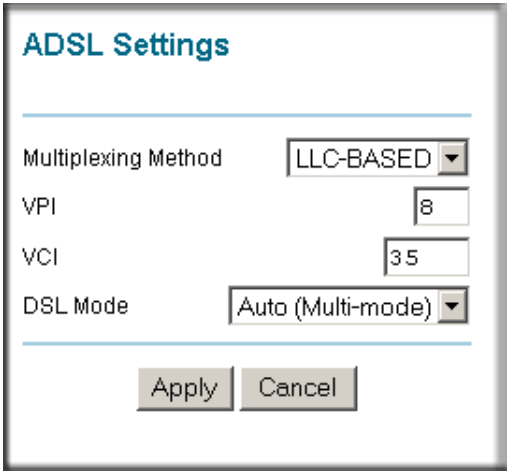



**Figure 3-14**

2. For the Multiplexing Method, select LLC-based or VC-based.
3. Type a number between 0 and 255 for the VPI. The default is 8.
4. Type a number between 1 and 65535 for the VCI. The default is 35.
5. Click **Apply**.

# Chapter 4
# Wireless Configuration

This chapter describes how to configure the wireless features of your 54 Mbps ADSL Modem Wireless Router Model DG834GSP.

## Considerations for a Wireless Network

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your modem router in order to maximize the network speed.

To ensure proper compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

### Observe Performance, Placement, and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless modem router. The latency, data throughput performance, and notebook power consumption also vary depending on your configuration choices.

| | |
|---|---|
| | **Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range/performance specifications, please see Appendix A, “Technical Specifications”. |

For best results, place your modem router:

- Near the center of the area in which your computers will operate
- In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls)
- Away from sources of interference, such as computers, microwaves, and cordless phones
- With the Antenna tight and in the upright position
- Away from large metal surfaces

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

## Implement Appropriate Wireless Security

| | |
|---|---|
| | **Note:** Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside of your immediate area to access your network. |

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The ADSL Modem Wireless Router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

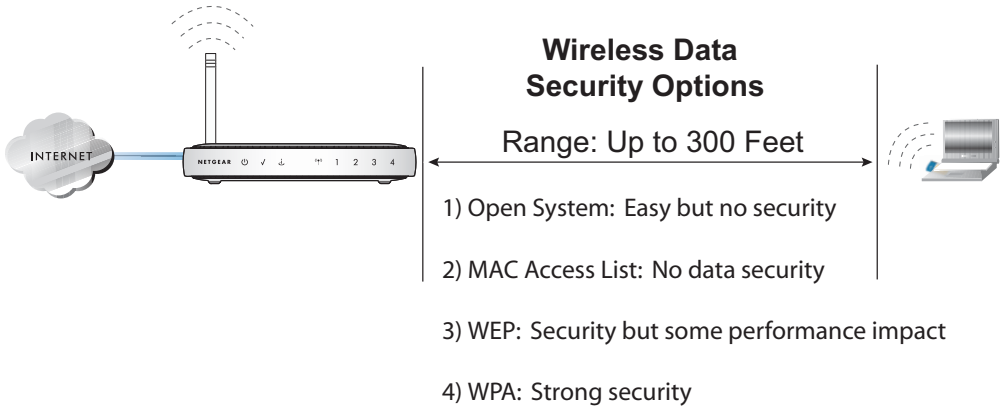

INTERNET
Wireless Data
Security Options
Range: Up to 300 Feet
1) Open System: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but some performance impact
4) WPA: Strong security

**Figure 4-1**

There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC Address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the DG834GSP. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network ‘discovery’ feature of some products, such as Windows XP, but the data is still exposed.

- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.
- **WPA-802.1x, WPA2-802.1x.** Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and RADIUS servers.
- **WPA-PSK (TKIP), WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA make it virtually impossible to compromise. Because this is a relatively new standard, wireless device driver and software availability may be limited.

# Understanding Wireless Settings

To configure the Wireless interface of your modem router, click the **Wireless Settings** link in the Setup section of the main menu. The Wireless Settings menu will appear, similar to that shown below:

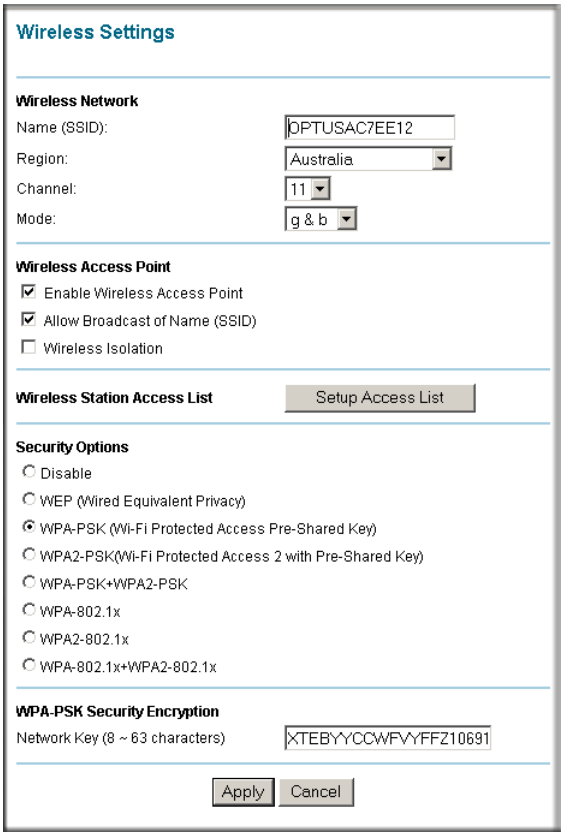



**Figure 4-2**

The following parameters are in the Wireless Settings menu:

- **Wireless Network**.
  - — **Name (SSID)**. The Service Set ID, also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. *The same Name (SSID) must be assigned to all wireless devices in your network*. The default SSID is a unique value printed on the label on the bottom of your modem router.

    **Note:** This value is case sensitive. For example, **Wireless** is not the same as **wireless**.

    Since your default SSID is unique, there is no good reason for changing its value. If you do change the value, performing a hard reset will restore the SSID to its default.

  - — **Region**. Select your country/region from the drop-down list. This field displays the region of operation for which the wireless interface is intended.
  - — **Channel**. This field determines which operating frequency will be used. The default channel is selected by encoding the MAC address. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.
  - — **Mode**. The default is "g & b", which allows both "g" and "b" wireless stations to access this device. “g only” allows only 802.11g wireless stations to be used. “b only” allows 802.11b wireless stations; 802.11g wireless stations can still be used if they can operate in 802.11b mode.
- **Wireless Access Point**.
  - — **Enable Wireless Access Point**. This field lets you turn off or turn on the wireless access point built in to the modem router. The wireless icon on the front of the modem router will also display the current status of the Wireless Access Point to let you know if it is disabled or enabled. The wireless access point must be enabled to allow wireless stations to access the Internet.
  - — **Allow Broadcast of Name (SSID)**. If enabled, the SSID is broadcast to all Wireless Stations. Stations that have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.
  - — **Wireless Isolation.** If enabled, Wireless Stations will not be able to communicate with each other or with Stations on the wired network. This feature should normally be disabled.

- **Wireless Station Access List**.
  - By default, any wireless computer that is configured with the correct wireless network name or SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only specific computers based on their MAC addresses. Click **Setup Access List** to display the Wireless Station Access List menu.
- **Security Options**

**Table 4-1. Wireless Security Options**

| Field | Description |
|---|---|
| **Disable** | Wireless security is not used. |
| **WEP** (Wired Equivalent Privacy) | You can select the following WEP options:<br><br>**Authentication Type**<br>• Open: the DG834GSP does not perform any authentication.<br>• Shared: WEP shared key authentication. For a full explanation of WEP shared key, see "Wireless Communications" in Appendix C.<br><br>**Encryption Strength**<br>• If Shared or Open Network Authentication is enabled, you can choose 64- or 128-bit WEP data encryption.<br>**Note**: With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the DG834GSP *does* perform 64- or 128-bit data encryption but *does not* perform any authentication.<br><br>**Security Encryption (WEP) Key**<br>These key values must be identical on all wireless devices in your network (key 1 must be the same for all, key 2 must be the same for all, and so on).<br>The DG834GSP provides two methods for creating WEP encryption keys:<br>• Passphrase. These characters *are* case sensitive. Enter a word or group of printable characters in the Passphrase box and click the **Generate** button.<br>**Note**: Not all wireless adapters support passphrase key generation.<br>• Manual. These values *are not* case sensitive.<br>64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F).<br>128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). |

**Table 4-1. Wireless Security Options (continued)**

| Field | Description |
|---|---|
| **WPA-PSK (TKIP), WPA2-PSK (AES)** | WPA Pre-Shared-Key (Wi-Fi Protected Access Pre-Shared Key) uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. WPA-PSK (TKIP) implements most of the IEEE 802.11i standard and is designed to work with all wireless network interface cards, but not all wireless access points. WPA2-PSK (AES) implements the full standard, but will not work with some older network cards. For a full explanation of WPA, see "Wireless Communications" in Appendix C.<br><br>By default, your unit is configured for WPA-PSK, which is the recommended encryption method to use with Windows Vista. |
| **WPA-802.1x, WPA2-802.1x** | User authentication is implemented using 802.1x and RADIUS servers. For a full explanation of WPA, see "Wireless Communications" in Appendix C.<br><br>Fill in the following:<br>• Radius Server Name/IP Address<br>This field is required. Enter the name or IP address of the Radius Server on your LAN.<br>• Radius Port<br>Enter the port number used for connections to the Radius Server.<br>• Radius Shared Key<br>Enter the desired value for the Radius shared key. This key enables the DG834GSP to log in to the Radius server and must match the value used on the Radius server. |

## How to Set Up and Test Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in to the DG834GSP modem router at its default LAN address of http://10.1.1.1 with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the **Wireless Settings** link in the main menu of the DG834GSP modem router.
3. Set the Region. Select the region in which the wireless interface will operate.
4. If necessary, set the Channel. The default channel is dependent on the MAC address.

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your modem router. For more information on the wireless channel frequencies please refer to "Wireless Communications" in Appendix C.

5. For initial configuration and test, leave the Wireless Card Access List set to allow everyone access by making sure that **Turn Access Control On** is not selected in the Wireless Station Access List. In addition, leave the Encryption Strength set to "Disabled."

6. Click **Apply** to save your changes.

**Note:** If you are configuring the modem router from a wireless computer and you change the modem router's SSID, channel, or security settings, you will lose your wireless connection when you click **Apply**. You must then change the wireless settings of your computer to match the modem router's new settings.

7. Configure and test your computers for wireless connectivity.

   Program the wireless adapter of your computers to have the same SSID and encryption type and passphrase as you configured in your modem router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the modem router.

Once your computers have basic wireless connectivity to the modem router, you can configure the advanced wireless security functions of the modem router.

## How to Restrict Wireless Access to Your Network

By default, any wireless PC that is configured with the correct SSID and WPA-PSK network key will be allowed access to your wireless network. This will be sufficient to deter all but the most determined hackers. The 54 Mbps ADSL Modem Wireless Router Model DG834GSP provides several ways to further restrict wireless access to your network:

- Turn off wireless connectivity completely
- Hiding your Wireless Network Name (SSID)
- Restrict access based on the Wireless Card Access List

These options are discussed below.

**Figure 4-3**

### Restricting Access to Your Network by Turning Off Wireless Connectivity

You can completely turn off the wireless portion of the DG834GSP. For example, if your notebook computer is used to wirelessly connect to your router and you take a business trip, you can turn off the wireless portion of the router while you are traveling. Other members of your household who use computers connected to the router via Ethernet cables will still be able to use the router.

### Hiding Your Wireless Network Name (SSID)

The DG834GSP can restrict wireless access to your network by not broadcasting the wireless network name (SSID). However, by default, this feature is turned off. If you turn this feature on, wireless devices will not ‘see’ your DG834GSP. You must configure your wireless devices to match the wireless network name (SSID) you configure in the ADSL Modem Wireless Router.

| | |
|---|---|
| | **Note:** The SSID of any wireless access adapters must match the SSID you configure in the 54 Mbps ADSL Modem Wireless Router Model DG834GSP. If they do not match, you will not get a wireless connection to the DG834GSP. |

### Restricting Wireless Access Based on the Wireless Station Access List

This list determines which wireless hardware devices will be allowed to connect to the modem router.

To restrict access based on MAC addresses, follow these steps:

1. Log in to the DG834GSP modem router at its default LAN address of http://10.1.1.1 with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

2. From the Wireless Settings menu, Wireless Station Access List section, click the **Setup Access List** button to display the list, shown below:

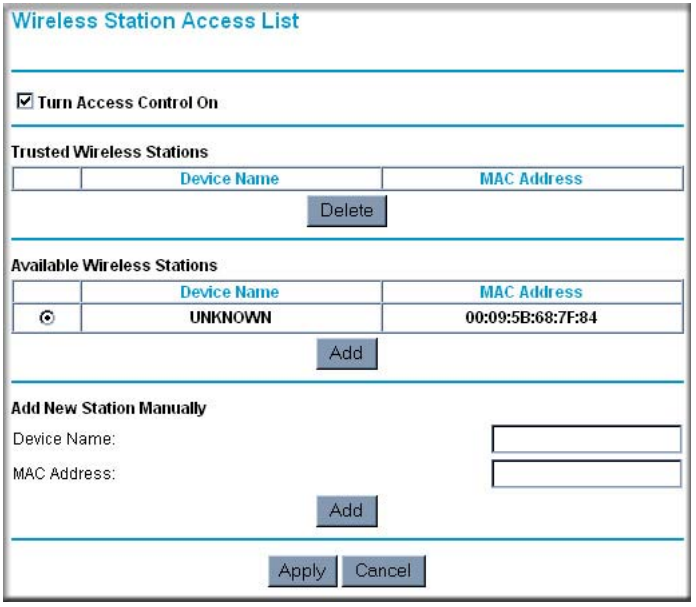



**Figure 4-4**

3. Select the **Turn Access Control On** check box to enable restricting wireless computers by their MAC addresses.
4. If the wireless station is currently connected to the network, you can select it from the Available Wireless Stations list. Click **Add** to add the station to the Trusted Wireless Stations list.
5. If the wireless station is not currently connected, you can enter its address manually. Enter the MAC address of the authorized computer. The MAC address is usually printed on the wireless card, or it may appear in the modem router's DHCP table. The MAC address will be 12 hexadecimal digits.

   Click **Add** to add your entry. You can add several stations to the list, but the entries will be discarded if you do not click **Apply**.

You can copy and paste the MAC addresses from the modem router's Attached Devices menu into the MAC Address box of this menu. To do this, configure each wireless computer to obtain a wireless link to the modem router. The computer should then appear in the Attached Devices menu.

**Note:** If you are configuring the modem router from a wireless computer whose MAC address is not in the Trusted Wireless Stations list, and you select **Trusted Wireless Stations only**, you will lose your wireless connection when you click **Apply**. You must then access the modem router from a wired computer to make any further changes.

6. Make sure the Turn Access Control On check box is selected, then click **Apply**.

Now, only devices on this list will be allowed to wirelessly connect to the DG834GSP. This prevents unauthorized access to your network.

## How to Configure WPA-PSK/WPA2-PSK Security

**Note:** The WPA-PSK key is printed on the bottom label. Not all wireless adapters support WPA. Consult the product document for your wireless adapter for instructions on configuring WPA settings.

To configure WPA-PSK or WPA2-PSK, follow these steps:

1. Log in at the default LAN address of http://10.1.1.1, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the Setup section of the main menu of the DG834GSP.
3. Choose the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK+WPA2-PSK** radio button. The **WPA-PSK+WPA2-PSK** option is the most flexible, as it allows wireless clients to use either WPA-PSK or WPA2-PSK protocol. The Security Encryption section will be displayed.
4. Enter the pre-shared key in the Passphrase field.
5. Click **Apply** to save your settings.

## How to Configure WPA-802.1x/WPA2-802.1x Security

**Note:** Not all wireless adapters support WPA. Consult the product document for your wireless adapter for instructions on configuring WPA settings.

To configure WPA-802.1x/WPA2-802.1x, follow these steps:

1. Log in at the default LAN address of http://10.1.1.1, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the Setup section of the main menu of the DG834GSP.
3. Choose the **WPA-802.1x**, **WA2-802.1x**, or **WPA-802.1x+WPA2-802.1x** radio button. The **WPA-802.1x+WPA2-802.1x** option is the most flexible, as it allows wireless clients to use either WPA-802.1x or WPA2-802.1x protocol.The page will display the WPA-802.1x/WPA2-802.1x section.
4. Enter the Radius server name/IP address.
5. Enter the Radius port number.
6. Enter the Shared Key.
7. Click **Apply** to save your settings.

# Choosing WEP Authentication and Security Encryption Methods

| | |
|---|---|
| | **Warning:** WEP is an older security standard than WPA and is easier to compromise. Only use this form of security if one or more of your wireless clients does not support WPA security. |

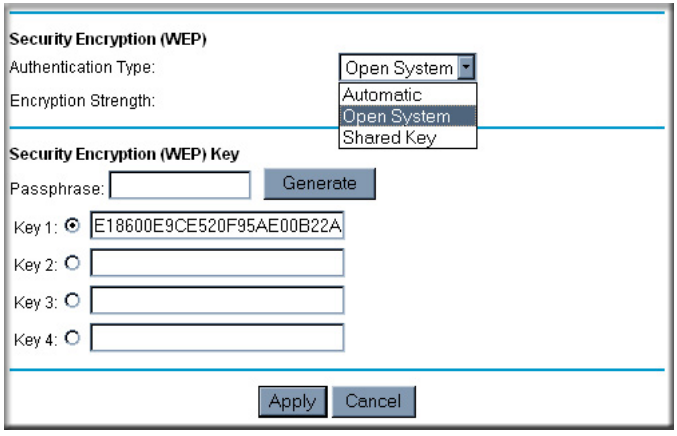



**Figure 4-5**

Restricting wireless access prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the WEP data encryption settings described below will prevent a determined intruder from eavesdropping on your wireless data communications. Also, if you are using the Internet for such activities as purchases or banking, those Internet sites use another level of highly secure encryption called SSL. You can tell if a web site is using SSL because the web address begins with HTTPS rather than HTTP.

### Authentication Type Selection

The DG834GSP lets you select the following wireless authentication schemes.

- Automatic
- Open System

- Shared key

| | |
|---|---|
| | **Note:** The authentication scheme is separate from the data encryption. You can choose an authentication scheme which requires a shared key but still leave the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings. |

Set your wireless adapter according to the authentication scheme you choose for the ADSL Modem Wireless Router. Please refer to "Wireless Communications" in Appendix C for a full explanation of each of these options, as defined by the IEEE 802.11g wireless communication standard.

### Encryption Choices

Please refer to "Wireless Communications" in Appendix C for a full explanation of each of the following choices, as defined by the IEEE 802.11g wireless communication standard. Choose the encryption strength from the drop-down list:

***Disable.*** No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.

***64 or 128 bit WEP.*** When 64 Bit WEP or 128 Bit WEP is selected, WEP encryption will be applied.

If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network.

There are two methods for creating WEP encryption keys:

- Passphrase. Enter a word or group of printable characters in the Passphrase box and click the **Generate** button.
- Manual. 64-bit WEP: Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: Enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

Select the radio button for the key you want to make active.

## How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the DG834GSP modem router at its default LAN address of http://10.1.1.1 with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the **Wireless Settings** link in the Setup section of the main menu for the DG834GSP modem router.
3. In the Security Options section, select the **WEP (Wired Equivalent Privacy)** radio button
4. Go to the WEP Security Encryption portion of the page:

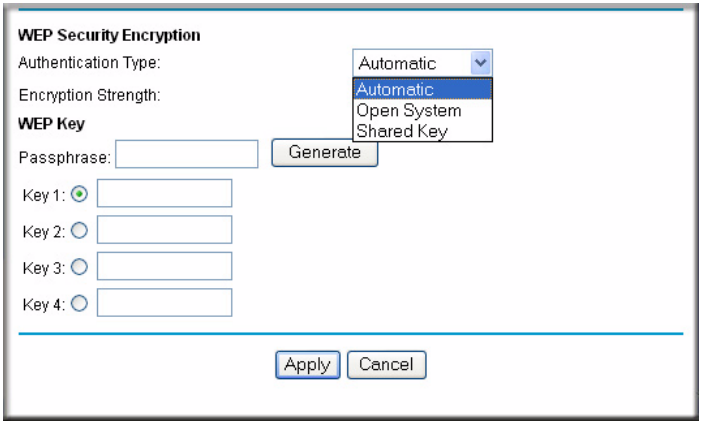



**Figure 4-6**

5. Select the **Authentication Type**.
6. Select the **Encryption Strength** setting.
7. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network.
   - Automatic — enter a word or group of printable characters in the Passphrase box and click the **Generate** button. The four key boxes will be automatically populated with key values.
   - Manual — enter hexadecimal digits (any combination of 0-9, a-f, or A-F). Select which of the four keys will be active.
8. Select the radio button for the key you want to make active.

   Be sure you clearly understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one included in Windows XP only allow entry of one key which must match the default key you set in the DG834GSP.

**9.** Click **Apply** to save your settings.

| | |
|---|---|
| | **Note:** When configuring the modem router from a wireless computer, if you configure WEP settings, you will lose your wireless connection when you click **Apply**. You must then either configure your wireless adapter to match the modem router WEP settings or access the modem router from a wired computer to make any further changes. |

# Chapter 5
# Protecting Your Network

This chapter describes how to use the basic firewall features of the 54 Mbps ADSL Modem Wireless Router Model DG834GSP to protect your network.

## Protecting Access to Your 54 Mbps ADSL Modem Wireless Router Model DG834GSP

For security reasons, the modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter **admin** for the modem router User Name and **password** for the modem router Password. You can use procedures below to change the modem router's password and the amount of time for the administrator's login timeout.

| | |
|---|---|
| | **Note:** The user name and password are not the same as any user name or password your may use to log in to your Internet connection. |

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

### How to Change the Built-In Password

1. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.

2. From the Main Menu of the browser interface, under the Maintenance heading, select **Set Password** to bring up the menu shown.

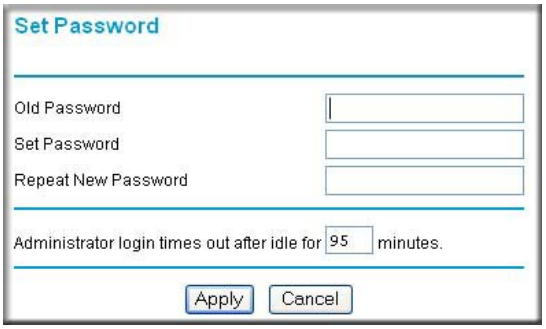



**Figure 5-1**

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

| | |
|---|---|
| | **Note:** After changing the password, you will be required to log in again to continue the configuration. If you have backed up the modem router settings previously, you should do a new backup so that the saved settings file includes the new password. |

## Changing the Administrator Login Timeout

For security, the administrator's login to the modem router configuration will timeout after a period of inactivity. To change the login timeout period:

1. In the Set Password menu, type a number in 'Administrator login times out' field. The suggested default value is 5 minutes.
2. Click **Apply** to save your changes or click **Cancel** to keep the current period.

# Configuring Basic Firewall Services

Basic firewall services include access blocking and scheduling of firewall security. These topics are presented below.

## Blocking Keywords, Sites, and Services

The modem router provides a variety of options for blocking Internet-based content and communications services. With its content filtering feature, the ADSL Modem Wireless Router prevents objectionable content from reaching your PCs. The modem router allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

- Keyword blocking of HTTP traffic.
- Outbound Service Blocking limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of Service (DoS) protection. Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

The section below explains how to configure your modem router to perform these functions.

## How to Block Keywords and Sites

The ADSL Modem Wireless Router allows you to restrict access to Internet content based on functions such as Web addresses and Web address keywords.

**1.** Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.

2. Select the **Block Sites** link of the Content Filtering menu.

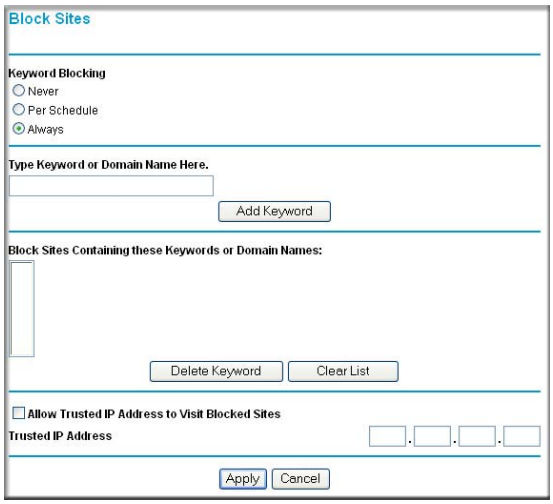



**Figure 5-2**

3. To enable keyword blocking, select one of the following:
   - **Per Schedule**—to turn on keyword blocking according to the settings on the Schedule page.
   - **Always**—to turn on keyword blocking all of the time, independent of the Schedule page.
4. Enter a keyword or domain in the Keyword box, click **Add Keyword**, then click **Apply**.

   Some examples of Keyword application follow:
   - If the keyword “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
   - If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
   - Enter the keyword “.” to block all Internet browsing access.

   Up to 32 entries are supported in the Keyword list.
5. To delete a keyword or domain, select it from the list, click **Delete Keyword**, then click **Apply**.
6. To specify a trusted user, enter that computer’s IP address in the Trusted IP Address box and click **Apply**.

You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.

7. Click **Apply** to save your settings.

## Firewall Rules

Firewall rules are used to block or allow specific traffic passing through from one side of the router to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the DG834GSP are:

- Inbound: Block all access from outside except responses to requests from the LAN side.
- Outbound: Allow all access from the LAN side to the outside.

You can define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

You can change the order of precedence of rules so that the rule that applies most often will take effect first. See “Order of Precedence for Rules” on page 5-11 for more details.

To access the rules configuration of the DG834GSP, click the **Firewall Rules** link on the main menu, then click **Add** for either an Outbound or Inbound Service.

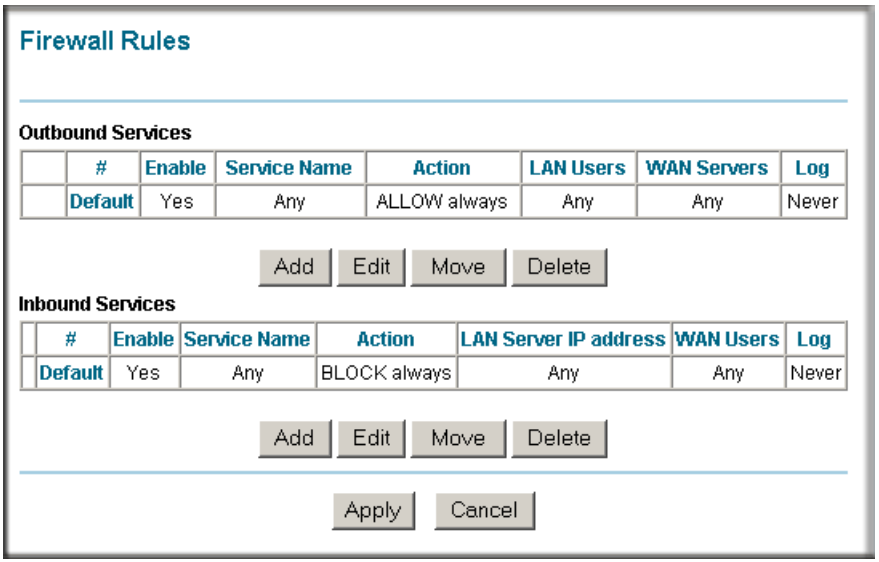

Firewall Rules
Outbound Services
# Enable Service Name Action LAN Users WAN Servers Log
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Inbound Services
# Enable Service Name Action LAN Server IP address WAN Users Log
Default Yes Any BLOCK always Any Any Never
Add Edit Move Delete
Apply Cancel

**Figure 5-3**

- To edit an existing rule, select its button on the left side of the table and click **Edit**.
- To delete an existing rule, select its button on the left side of the table and click **Delete**.
- To move an existing rule to a different position in the table, select its button on the left side of the table and click **Move**. At the script prompt, enter the number of the desired new position and click **OK**.

# Inbound Rules (Port Forwarding)

Because the DG834GSP uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the modem router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

**Note:** Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

### Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day. This rule is shown:

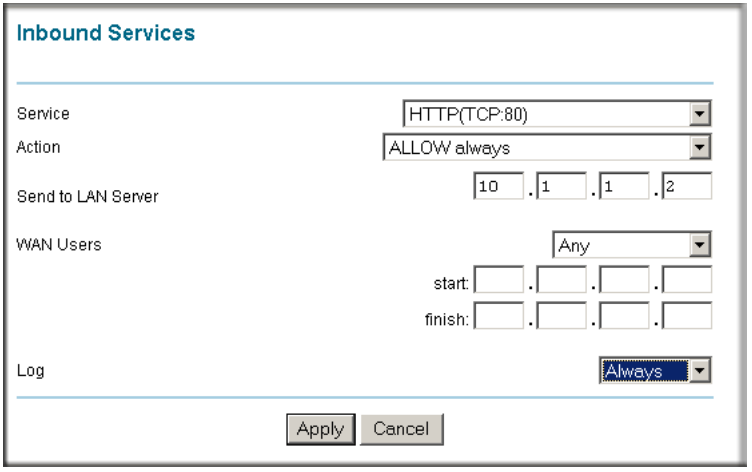



**Figure 5-4**

The parameters are:

- **Service—**From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services menu to add any additional services or applications that do not already appear.
- **Action—**Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **Send to LAN Server—**Enter the IP address of the computer or server on your LAN which will receive the inbound traffic covered by this rule.
- **WAN Users—**These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:
  - Any — all IP addresses are covered by this rule.
  - Address range — if this option is selected, you must enter the **Start** and **Finish** fields.
  - Single address — enter the required address in the Start field.
- **Log—**You can select whether the traffic will be logged. The choices are:
  - **Never** — no log entries will be made for this service.
  - **Always** — any traffic for this service type will be logged.
  - **Match** — traffic of this type which matches the parameters and action will be logged.
  - **Not match** — traffic of this type which does not match the parameters and action will be logged.

### Considerations for Inbound Rules

If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menu so that external users can always find your network.

If the IP address of the local server computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer's IP address constant.

Local computers must access the local server using the server's local LAN address (10.1.1.2 in the example above). Attempts by local computers to access the server using the external WAN IP address will fail.

# Outbound Rules (Service Blocking)

The DG834GSP allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on:

- IP address of the local computer (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Following is an application example of outbound rules.

## Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the modem router log any attempt to use Instant Messenger during that blocked period.

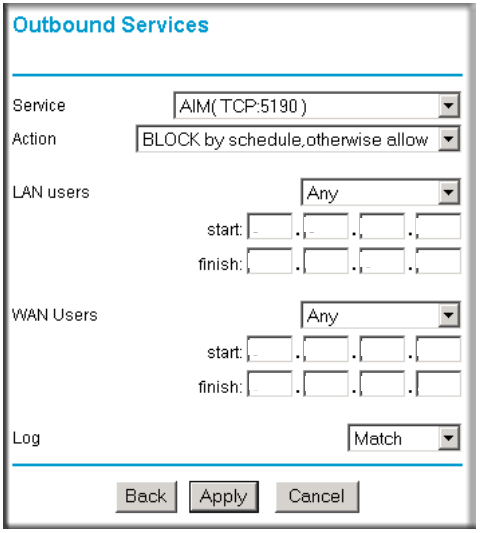


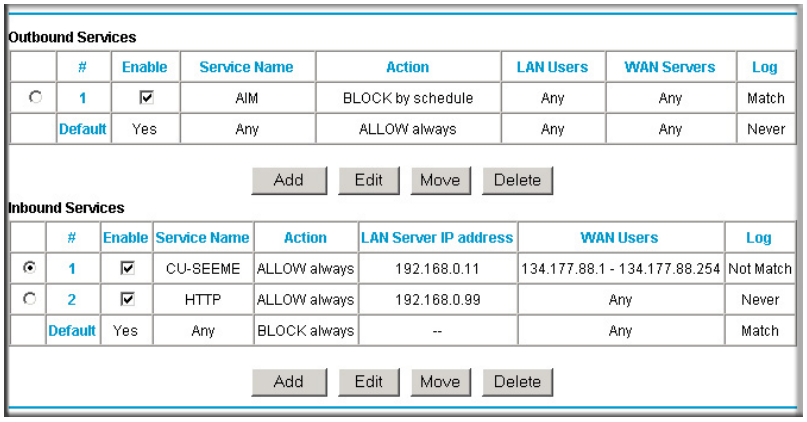

**Figure 5-5**

The parameters are:

- **Service—**From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Add Custom Service feature to add any additional services or applications that do not already appear; see "How to Define Services" on page 5-12 for details.
- **Action—**Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **LAN Users—**These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:
  - **Any** — all IP addresses are covered by this rule.
  - **Address range** — if this option is selected, you must enter the **Start** and **Finish** fields.
  - **Single address** — enter the required address in the Start field.
- **WAN Users—**These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the desired option:
  - **Any** — all IP addresses are covered by this rule.
  - **Address range** —if this option is selected, you must enter the Start and Finish fields.
  - **Single address** — enter the required address in the Start field.
- **Log—**You can select whether the traffic will be logged. The choices are:
  - **Never** — no log entries will be made for this service.
  - **Always** — any traffic for this service type will be logged.
  - **Match** — traffic of this type that matches the parameters and action will be logged.
  - **Not match** — traffic of this type that does not match the parameters and action will be logged.

## Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown:



Outbound Services

| | # | Enable | Service Name | Action | LAN Users | WAN Servers | Log |
|---|---|---|---|---|---|---|---|
| ○ | 1 | ☑ | AIM | BLOCK by schedule | Any | Any | Match |
| | Default | Yes | Any | ALLOW always | Any | Any | Never |

Add Edit Move Delete

Inbound Services

| | # | Enable | Service Name | Action | LAN Server IP address | WAN Users | Log |
|---|---|---|---|---|---|---|---|
| ◉ | 1 | ☑ | CU-SEEME | ALLOW always | 192.168.0.11 | 134.177.88.1 - 134.177.88.254 | Not Match |
| ○ | 2 | ☑ | HTTP | ALLOW always | 192.168.0.99 | Any | Never |
| | Default | Yes | Any | BLOCK always | -- | Any | Match |

Add Edit Move Delete

**Figure 5-6**

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

# Services

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the DG834GSP already holds a list of many service port numbers, you are not limited to these choices. Use the procedure below to create your own service definitions.

## How to Define Services

1. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.
2. Select the **Services** link of the Content Filtering menu to display the Services menu shown:

**Figure 5-7**

- To create a new Service, click the **Add Custom Service** button.
- To edit an existing Service, select its button on the left side of the table and click **Edit Service**.
- To delete an existing Service, select its button on the left side of the table and click **Delete Service**.

3. Use the page shown below to define or edit a service.

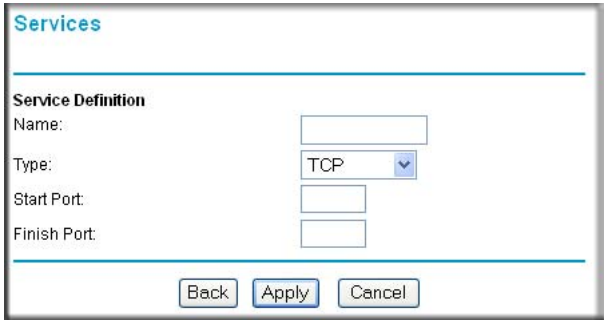



**Figure 5-8**

4. Click **Apply** to save your changes.

# Setting Times and Scheduling Firewall Services

The ADSL Modem Wireless Router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet.

## How to Set Your Time Zone

In order to localize the time for your log entries, you must specify your Time Zone:

1. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.
2. Select the **Schedule** link of the Content Filtering menu to display menu shown below.

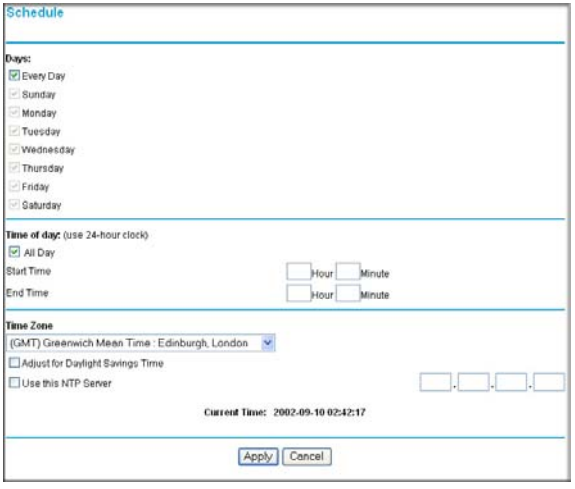



**Figure 5-9**

3. Select your time zone. This setting will be used for the blocking schedule according to your local time zone and for time-stamping log entries.

Select the **Adjust for daylight savings time** check box if your time zone is currently in daylight savings time.

| | |
|---|---|
| | **Note:** If your region uses Daylight Savings Time, you must manually select **Adjust for Daylight Savings Time** on the first day of Daylight Savings Time, and clear it at the end. Enabling Daylight Savings Time will cause one hour to be added to the standard time. |

4. The modem router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, enter its IP address under Use this NTP Server.
5. Click **Apply** to save your settings.

## How to Schedule Firewall Services

If you enabled services blocking in the Block Services menu or Port forwarding in the Ports menu, you can set up a schedule for when blocking occurs or when access is not restricted.

1. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.
2. Select the **Schedule** link of the Content Filtering menu to display menu shown above.
3. To block Internet services based on a schedule, select **Every Day** or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, enter Start Blocking and End Blocking times.
4. Enter the values in 24-hour time format. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.
5. Click **Apply** to save your changes.

# Chapter 6
# Managing Your Network

This chapter describes how to perform network management tasks with your 54 Mbps ADSL Modem Wireless Router Model DG834GSP.

## Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the ADSL Modem Wireless Router are stored in a configuration file in the modem router. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.

### How to Back Up the Configuration to a File

1. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the modem router.
2. From the Maintenance heading of the Main Menu, select the **Backup Settings** menu shown.

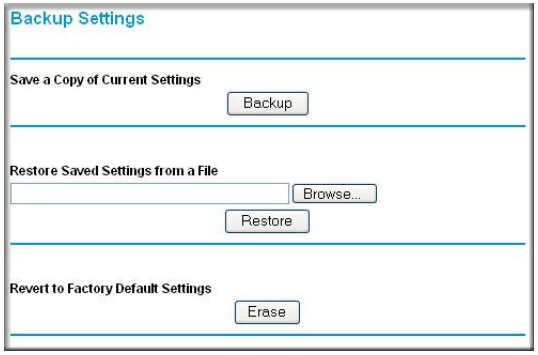



**Figure 6-1**

3. Click **Backup** to save a copy of the current settings.
4. Store the `.cfg` file on a computer on your network.

## How to Restore the Configuration from a File

1. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the modem router.
2. From the Maintenance heading of the Main Menu, select the **Settings Backup** menu.
3. Enter the full path to the file on your network or click the **Browse** button to locate the file.
4. When you have located the `.cfg` file, click the **Restore** button to upload the file to the modem router.
5. The modem router will then reboot automatically.

## How to Erase the Configuration

It is sometimes desirable to restore the modem router to the factory default settings. This can be done by using the Erase function.

1. To erase the configuration, from the Maintenance menu Settings Backup link, click the **Erase** button on the screen.
2. The modem router will then reboot automatically.

   After an erase, the modem router's password will be **password**, the LAN IP address will be 10.1.1.1, and the modem router's DHCP client will be enabled.

| | |
|---|---|
| | **Note:** To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the modem router. See "The Router's Rear Panel" on page 2-9. |

# Upgrading the Modem Router's Firmware

The software of the ADSL Modem Wireless Router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

Upgrade files can be downloaded from NETGEAR's Web site. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN or .IMG) file before uploading it to the modem router.

## How to Upgrade the Modem Router Firmware

NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you may need to restore your configuration settings.

1. Download and unzip the new software file from NETGEAR.

   The Web browser used to upload new firmware into the modem router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or above, or Netscape Navigator 4.7 or above.

2. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the modem router.

3. From the Main Menu of the browser interface, under the Maintenance heading, select the **Router Upgrade** heading to display the menu shown.

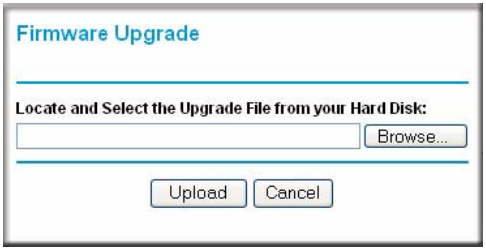



**Figure 6-2**

4. In the Router Upgrade menu, click **Browse** to locate the binary (.BIN or .IMG) upgrade file.
5. Click **Upload**.

| | |
|---|---|
| ⚠ | **Warning:** When uploading software to the modem router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your modem router will automatically restart. The upgrade process will typically take about one minute. In some cases, you may need to clear the configuration and reconfigure the modem router after upgrading. |

# Network Management Information

The DG834GSP provides a variety of status and usage information which is discussed below.

## Viewing Modem Router Status and Usage Statistics

From the Main Menu, under Maintenance, click **Router Status** to view this screen.

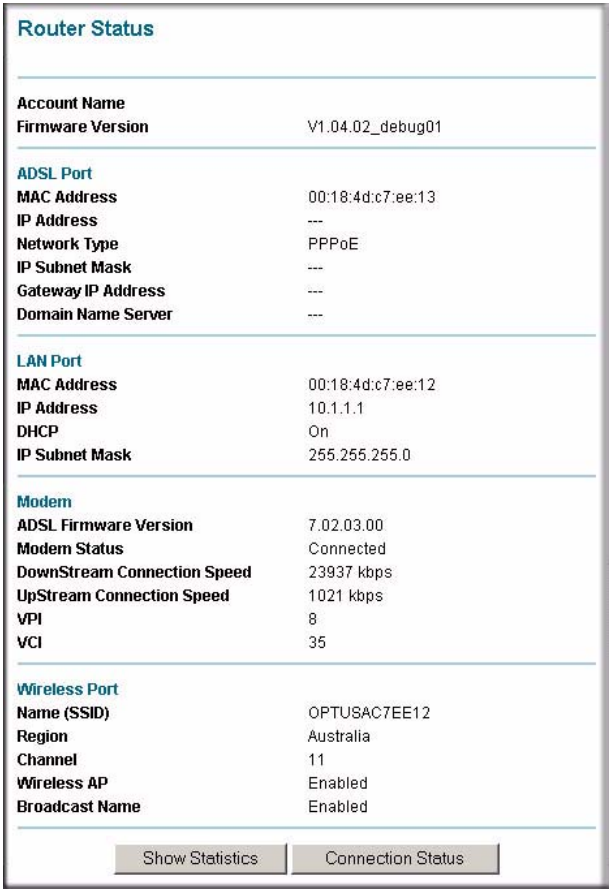



**Figure 6-3**

The Modem Router Status menu provides status and usage information.

This screen shows the following parameters:

**Table 6-1. Menu 3.2 - Modem Router Status Fields**

| Field | Description |
|---|---|
| Account Name | The Host Name assigned to the modem router in the Basic Settings menu. |
| Firmware Version | This field displays the modem router firmware version. |
| ADSL Port | These parameters apply to the Internet (ADSL) port of the modem router. |
| MAC Address | This field displays the Ethernet MAC address being used by the Internet (ADSL) port of the modem router. |
| IP Address | This field displays the IP address being used by the Internet (ADSL) port of the modem router. If no address is shown, the modem router cannot connect to the Internet. |
| Network Type | The network type depends is determined by your ISP. Common network types are PPPoE and PPPoA. |
| IP Subnet Mask | This field displays the IP Subnet Mask being used by the Internet (ADSL) port of the modem router. |
| Domain Name Server (DNS) | This field displays the DNS Server IP addresses being used by the modem router. These addresses are usually obtained dynamically from the ISP. |
| LAN Port | These parameters apply to the Local (ADSL) port of the modem router. |
| MAC Address | This field displays the Ethernet MAC address being used by the Local (LAN) port of the modem router. |
| IP Address | This field displays the IP address being used by the Local (LAN) port of the modem router. The default is 10.1.1.1. |
| DHCP | If OFF, the modem router will not assign IP addresses to PCs on the LAN.<br>If ON, the modem router will assign IP addresses to PCs on the LAN. |
| IP Subnet Mask | This field displays the IP Subnet Mask being used by the Local (LAN) port of the modem router. The default is 255.255.255.0. |
| Modem | These parameters apply to the Local (WAN) port of the modem router. |

**Table 6-1. Menu 3.2 - Modem Router Status Fields (continued)**

| Field | Description |
|---|---|
| ADSL Firmware Version | The version of the firmware. |
| Modem Status | The connection status of the modem. |
| Downstream Speed | The speed at which the modem is receiving data from the ADSL line. |
| Upstream Speed | The speed at which the modem is transmitting data to the ADSL line. |
| VPI | The Virtual Path Identifier setting. |
| VCI | The Virtual Channel Identifier setting. |
| Wireless Port | These are the settings as set in the Wireless Settings page; see "Understanding Wireless Settings" in Chapter 4 for details. |
| Name (SSID) | The Service Set ID, also known as the wireless network name. |
| Region | The country where the unit is set up for use. |
| Channel | The current channel, which determines the operating frequency. |
| Wireless AP | Indicates if the Access Point feature is disabled or not. If not enabled, the Wireless LED on the front panel will be off. |
| Broadcast Name | Indicates if the DG834GSP is configured to broadcast its SSID. |

Click the **Show Statistics** button to display modem router usage statistics, as shown below:

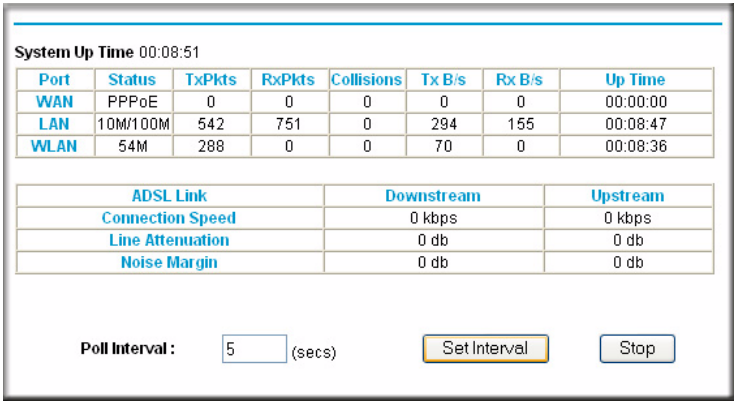

System Up Time 00:08:51
Port Status TxPkts RxPkts Collisions Tx B/s Rx B/s Up Time
WAN PPPoE 0 0 0 0 0 00:00:00
LAN 10M/100M 542 751 0 294 155 00:08:47
WLAN 54M 288 0 0 70 0 00:08:36
ADSL Link Downstream Upstream
Connection Speed 0 kbps 0 kbps
Line Attenuation 0 db 0 db
Noise Margin 0 db 0 db
Poll Interval : 5 (secs) Set Interval Stop

**Figure 6-4**

This screen shows the following statistics:

**Table 6-2. Router Statistics Fields**

| Field | Description |
|---|---|
| WAN or LAN Port | The statistics for the WAN (Internet) and LAN ports. |
| Status | The link status of the port. |
| TxPkts | The number of packets transmitted on this port since reset or manual clear. |
| RxPkts | The number of packets received on this port since reset or manual clear. |
| Collisions | The number of collisions on this port since reset or manual clear. |
| Tx B/s | The current line utilization—percentage of current bandwidth used on this port. |
| Rx B/s | The average line utilization for this port. |
| Up Time | The time elapsed since the last power cycle or reset. |
| ADSL Link Downstream or Upstream | The statistics for the upstream and downstream ADSL link. These statistics will be of interest to your technical support representative if you are having problems obtaining or maintaining a connection. |
| Connection Speed | Typically, the downstream speed is faster than the upstream speed. |
| Line Attenuation | The line attenuation will increase the further you are physically located from your ISP's facilities. |
| Noise Margin | This is the signal-to-noise ratio and is a measure of the quality of the signal on the line. |
| Poll Interval | Specifies the interval at which the statistics are updated in this window. Click **Stop** to freeze the display. |

Click the **Connection Status** button to display modem router connection status, shown below:

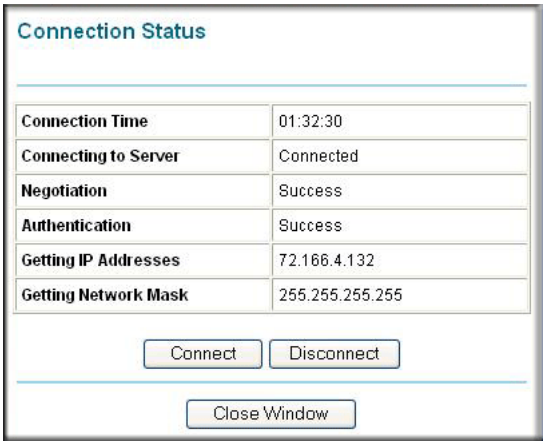



**Figure 6-5**

This screen shows the following statistics:

**Table 6-3. Connection Status Fields for PPPoA**

| Field | Description |
|---|---|
| Connection Time | The time elapsed since the last connection to the Internet via the ADSL port. |
| Connecting to Sender | The connection status. |
| Negotiation | ON or OFF |
| Authentication | ON or OFF |
| IP Address | The IP Address assigned to the WAN port by the ADSL Internet Service Provider. |
| Network Mask | The Network Mask assigned to the WAN port by the ADSL Internet Service Provider. |

## Viewing Attached Devices

The Attached Devices menu contains a table of all IP devices that the modem router has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select **Attached Devices** to view the table, shown:

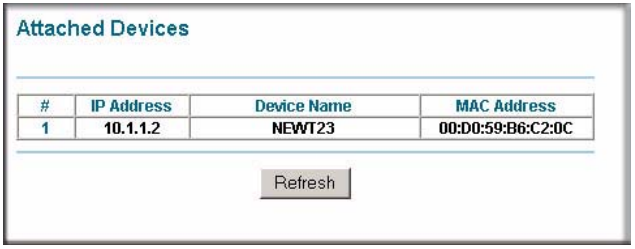



**Figure 6-6**

For each device, the table shows the IP address, Device Name if available, and the Ethernet MAC address. Note that if the modem router is rebooted, the table data is lost until the modem router rediscovers the devices. To force the modem router to look for attached devices, click the **Refresh** button.

## Viewing, Selecting, and Saving Logged Information

The modem router will log security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites menu, the Logs page can show you when someone on your network tries to access a blocked site. If you enabled e-mail notification, you will receive these logs in an e-mail message. If you do not have e-mail notification enabled, you can view the logs here.

An example of the logs file is shown below.

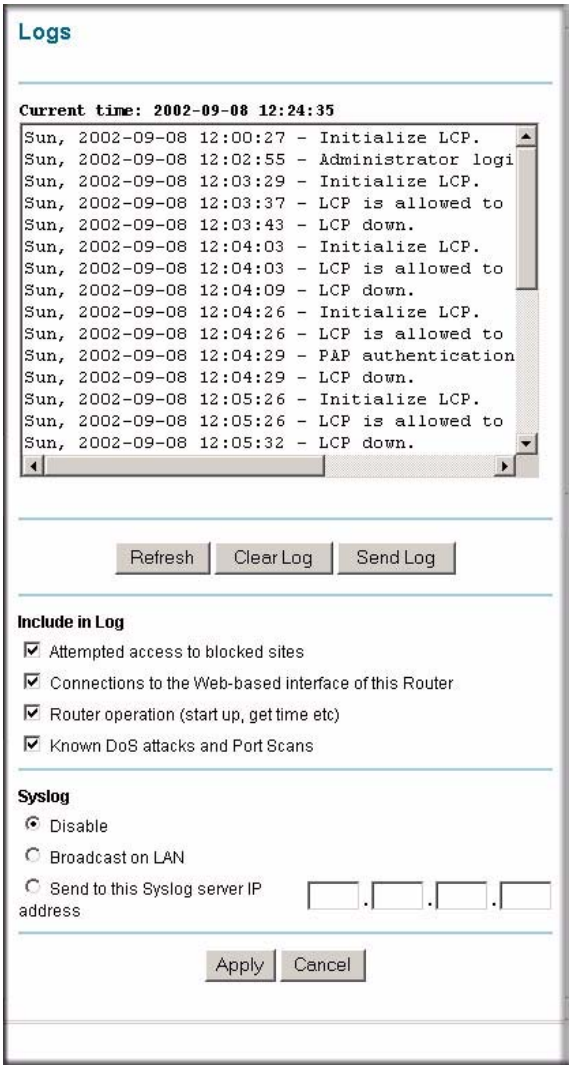

Logs
Current time: 2002-09-08 12:24:35
Sun, 2002-09-08 12:00:27 - Initialize LCP.
Sun, 2002-09-08 12:02:55 - Administrator logi
Sun, 2002-09-08 12:03:29 - Initialize LCP.
Sun, 2002-09-08 12:03:37 - LCP is allowed to
Sun, 2002-09-08 12:03:43 - LCP down.
Sun, 2002-09-08 12:04:03 - Initialize LCP.
Sun, 2002-09-08 12:04:03 - LCP is allowed to
Sun, 2002-09-08 12:04:09 - LCP down.
Sun, 2002-09-08 12:04:26 - Initialize LCP.
Sun, 2002-09-08 12:04:26 - LCP is allowed to
Sun, 2002-09-08 12:04:29 - PAP authentication
Sun, 2002-09-08 12:04:29 - LCP down.
Sun, 2002-09-08 12:05:26 - Initialize LCP.
Sun, 2002-09-08 12:05:26 - LCP is allowed to
Sun, 2002-09-08 12:05:32 - LCP down.
Refresh
Clear Log
Send Log
Include in Log
Attempted access to blocked sites
Connections to the Web-based interface of this Router
Router operation (start up, get time etc)
Known DoS attacks and Port Scans
Syslog
Disable
Broadcast on LAN
Send to this Syslog server IP address
Apply
Cancel

**Figure 6-7**

Log entries are described in Table 6-4 below:

**Table 6-4. Security Log entry descriptions**

| Field | Description |
|---|---|
| Date and Time | The date and time the log entry was recorded. |
| Description or Action | The type of event and what action was taken if any. |
| Source IP | The IP address of the initiating device for this log entry. |
| Source port and interface | The service port number of the initiating device, and whether it originated from the LAN or WAN |
| Destination | The name or IP address of the destination device or Web site. |
| Destination port and interface | The service port number of the destination device, and whether it's on the LAN or WAN. |

Log action buttons are described in Table 6-5 below:

**Table 6-5. Security Log action buttons**

| Field | Description |
|---|---|
| Refresh | Refresh the log screen. |
| Clear Log | Clear the log entries. |
| Send Log | Email the log immediately. |
| Apply | Apply the current settings. |
| Cancel | Clear the current settings. |

### Selecting What Information to Log

Besides the standard information listed above, you can choose to log additional information. Those optional selections are as follows:

- Attempted access to blocked site
- Connections to the Web-based interface of the modem router
- Modem Router operation (start up, get time, etc.)
- Known DoS attacks and Port Scans

### Saving Log Files on a Server

You can choose to write the logs to a computer running a syslog program. To activate this feature, select to Broadcast on Lan or enter the IP address of the server where the Syslog file will be written.

## Examples of Log Messages

Following are examples of log messages. In all cases, the log entry shows the timestamp as: Day, Year-Month-Date Hour:Minute:Second.

### Activation and Administration

```
Tue, 2002-05-21 18:48:39 - NETGEAR activated
```

[This entry indicates a power-up or reboot with initial time entry.]

```
Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:10.1.1.2
Thu, 2002-05-21 18:56:58 - Administrator logout - IP:10.1.1.2
```

[This entry shows an administrator logging in and out from IP address 10.1.1.2.]

```
Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:10.1.1.2
```

[This entry shows a time-out of the administrator login.]

```
Wed, 2002-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was emailed.]

### Dropped Packets

```
Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

[These entries show an inbound FTP (port 21) packet, User Datagram Protocol (UDP) packet (port 6970), and Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

## Enabling Security Event E-mail Notification

In order to receive logs and alerts by e-mail, you must provide your e-mail information in the E-mail heading in the Content Filtering section of the main menu:

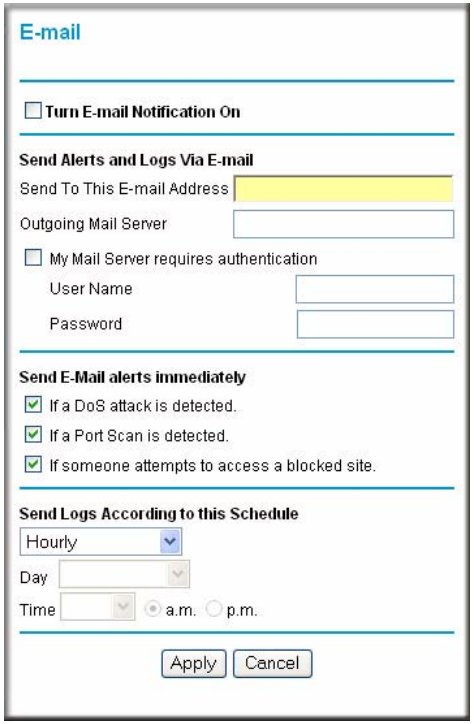



**Figure 6-8**

- **Turn e-mail notification on**. Select this check box if you want to receive e-mail logs and alerts from the modem router.
- **Send alerts and logs via email**.
  - **Send To This E-mail Address** Enter the e-mail address where you want to send the alerts and logs. Use a full e-mail address, such as ChrisXY@myISP.com.
  - **Outgoing Mail Server**. Enter the name or IP address of the outgoing SMTP mail server of your ISP (such as mail.myISP.com).
  - Check **My Mail Server requires authentication** if you need to login to your SMTP server to send E-mail. If you check this box, you must enter the user name and password for the mail server.

**Tip:** If you cannot remember the above information from when you set up your e-mail account, check the settings in your e-mail program.

- **Send alert immediately.** Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule.** Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - Day for sending log
    Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
  - Time for sending log
    Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot e-mail the log file, the log buffer may fill up. In this case, the modem router overwrites the log and discards its contents.

# Running Diagnostic Utilities and Rebooting the Modem Router

The ADSL Modem Wireless Router has a diagnostics feature. You can use the diagnostics menu to perform the following functions from the modem router:

- Ping an IP Address to test connectivity to see if you can reach a remote host. If Ping VPN is enabled, the ping packet always goes through the VPN if the VPN tunnel is enabled and working.
- Perform a DNS Lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing Table to identify what other modem routers the modem router is communicating with.
- Reboot the modem router to enable new network configurations to take effect or to clear problems with the modem router's network connection.

From the Main Menu of the browser interface, under the Maintenance heading, select the **Modem Router Diagnostics** heading to display the menu shown.

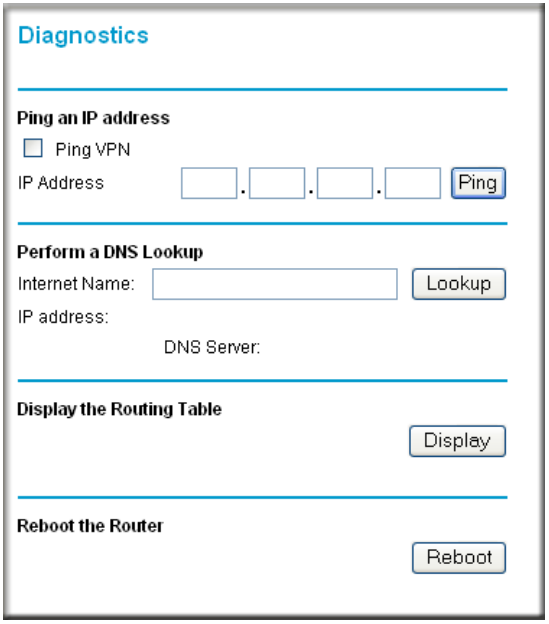



**Figure 6-9**

# Enabling Remote Management

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your 54 Mbps ADSL Modem Wireless Router Model DG834GSP.

**Tip:** Be sure to change the modem router's default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters.

## Configuring Remote Management

1. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the modem router.
2. From the Advanced section of the main menu, select the **Remote Management** link.

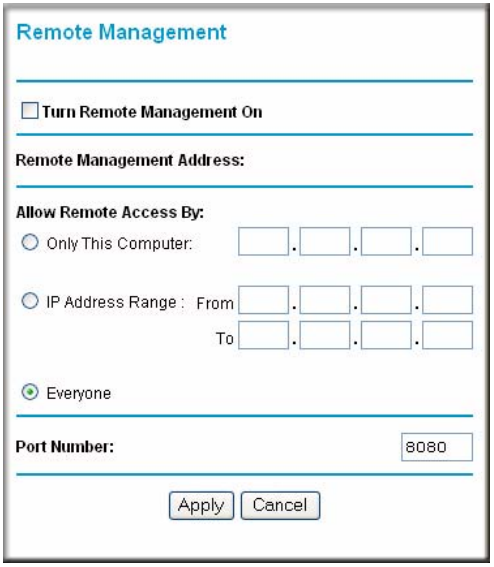



**Figure 6-10**

3. Select the **Turn Remote Management On** check box.

4. Specify what external addresses will be allowed to access the modem router's remote management.
   For security, restrict access to as few external IP addresses as practical:
   - To allow access from any IP address on the Internet, select **Everyone**.
   - To allow access from a range of IP addresses on the Internet, select **IP address range**. Enter a beginning and ending IP address to define the allowed range.
   - To allow access from a single IP address on the Internet, select **Only this Computer**. Enter the IP address that will be allowed access.
5. Specify the Port Number that will be used for accessing the management interface.

   Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
6. Click **Apply** to have your changes take effect.

   When accessing your modem router from the Internet, you will type your modem router's WAN IP address in your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter in your browser:

   ```
   http://134.177.0.123:8080
   ```

| | |
|---|---|
| | **Note:** In this case, the http:// must be included in the address. |

# Chapter 7
# Advanced Configuration

This chapter describes how to configure the advanced features of your 54 Mbps ADSL Modem Wireless Router Model DG834GSP.

## Configuring Advanced Security

The 54 Mbps ADSL Modem Wireless Router Model DG834GSP provides a variety of advanced features, such as:

- Setting up a Demilitarized Zone (DMZ) Server
- Connecting Automatically, as Required
- Disabling Port Scan and DOS Protection
- Responding to a Ping on the Internet WAN Port
- MTU Size
- Flexibility on configuring your LAN TCP/IP settings
- Using the Router as a DHCP Server
- Configuring Dynamic DNS
- Configuring Static Routes
- Wireless Bridging and Repeating

These features are discussed below.

# Setting Up A Default DMZ Server

The Default DMZ Server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The modem router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the Default DMZ Server.

**Warning:** For security reasons, you should avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

## How to Configure a Default DMZ Server

To assign a computer or server to be a Default DMZ server, follow these steps:

1. Log in to the modem router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.

2. From the Main Menu, under Advanced, click the **WAN Setup** link to view the page shown:

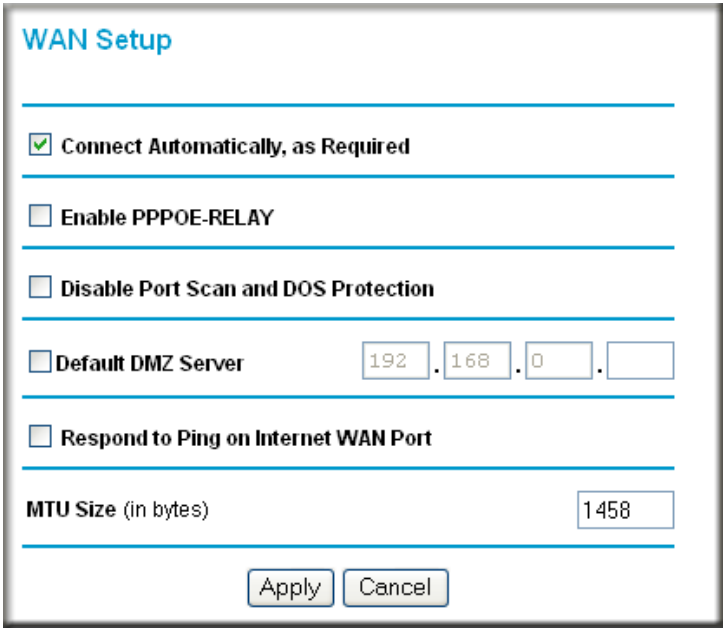



**Figure 7-1**

3. Select the **Default DMZ Server** check box.
4. Type the IP address for that server.
5. Click **Apply** to save your changes.

## Connect Automatically, as Required

Normally, this option should be enabled, so that an Internet connection will be made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting.

If disabled, you must connect manually, using the sub-screen accessed from the "Connection Status" button on the Status screen.

If you have an "Always on" connection, this setting has no effect.

## Enable PPPoE-Relay

When enabled, this feature allows a PPPoE client on a local PC to a remote PPPoE server with the gateway acting as a relay agent.

## Disable Port Scan and DOS Protection

The Firewall protects your LAN against Port Scans and Denial of Service (DOS) attacks. This should be disabled only in special circumstances.

## Respond to Ping on Internet WAN Port

If you want the modem router to respond to a 'ping' from the Internet, select the **Respond to Ping on Internet WAN Port** check box. This should only be used as a diagnostic tool, since it allows your modem router to be discovered. Do not select this box unless you have a specific reason to do so.

## MTU Size

The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, or 1492 Bytes for PPPoE connections. For some ISPs you may need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

# Configuring LAN IP Settings

The LAN IP Setup menu allows configuration of LAN IP services such as DHCP and RIP. These features can be found under the Advanced heading in the Main Menu of the browser interface.

The modem router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The modem router's default LAN IP configuration is:

- LAN IP addresses—10.1.1.1
- Subnet mask—255.255.255.0

These addresses are part of the Internet Engineering Task Force (IETF)-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

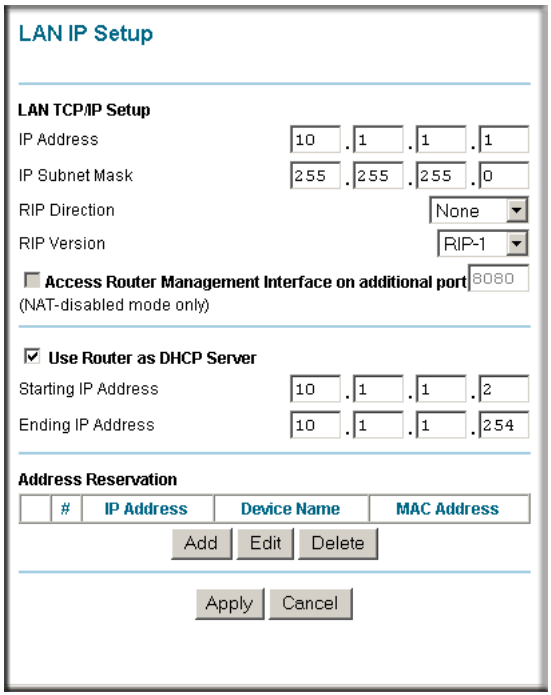



**Figure 7-2**

The LAN TCP/IP Setup parameters are:

- IP Address
  This is the LAN IP address of the modem router.

| | |
|---|---|
| ⚠ | **Warning:** If you change the LAN IP address of the modem router while connected through the browser, you or anyone else using the router will be disconnected. You must then open a new connection to the new IP address and log in again. Others using the router will have to restart their computer and connect to the router again. |

- IP Subnet Mask
  This is the LAN Subnet Mask of the modem router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router.
- RIP Direction
  RIP (Router Information Protocol) allows a modem router to exchange routing information with other routers. The RIP Direction selection controls how the Modem Router sends and receives RIP packets. Both is the default.
  - When set to Both or Out Only, the modem router will broadcast its routing table periodically.
  - When set to Both or In Only, it will incorporate the RIP information that it receives.
  - When set to None, it will not send any RIP packets and will ignore any RIP packets received.
- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the modem router sends. It recognizes both formats when receiving. By default, this is set for RIP-1.
  - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
  - RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
    - RIP-2B uses subnet broadcasting.
    - RIP-2M uses multicasting.
- Access Router Management Interface on additional port.
  This option is only available if you have disabled Network Address Translation and you have been assigned a static address by your ISP. This allows your router to be managed remotely on a specially assigned port instead of the HTTP port (80).

## DHCP

By default, the modem router will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the modem router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See "Internet Networking and TCP/IP Addressing" in Appendix C for an explanation of DHCP and information about how to assign IP addresses for your network.

### Use Router as DHCP server

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the 'Use router as DHCP server' check box. Otherwise, leave it selected.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 10.1.1.2 and 10.1.1.254, although you may want to save part of the range for devices with fixed addresses.

The router will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address is the router's LAN IP address
- Primary DNS Server, if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router's LAN IP address
- Secondary DNS Server, if you entered a Secondary DNS address in the Basic Settings menu
- WINS Server, short for *Windows Internet Naming Service Server,* determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

### Reserved IP addresses

When you specify a reserved IP address for a computer on the LAN, that computer will always receive the same IP address each time it access the router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

**1.** Click the **Add** button.

2. In the IP Address box, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 10.1.1.x.
3. Type the MAC Address of the computer or server.

**Tip:** If the computer is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.

4. Click **Apply** to enter the reserved address into the table.

**Note:** The reserved address will not be assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

## How to Configure LAN TCP/IP Settings

1. Log in to the router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.

2. From the Main Menu, under Advanced, click the **LAN IP Setup** link to view the menu, shown:

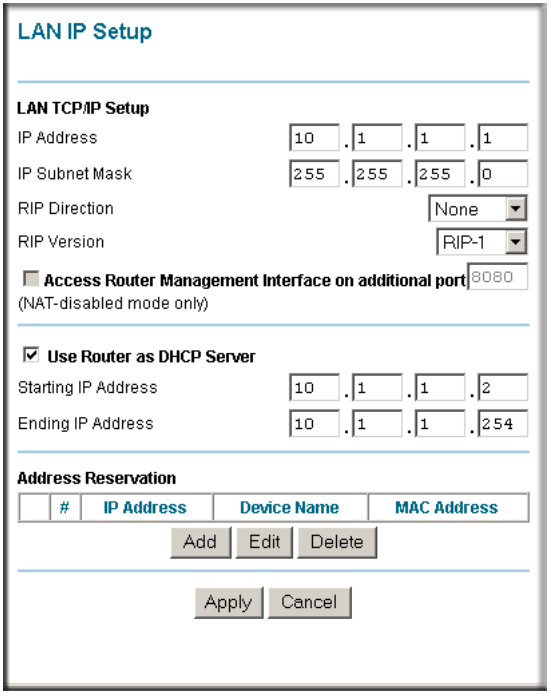



**Figure 7-3**

3. Enter the TCP/IP, DHCP, or Reserved IP parameters.
4. Click **Apply** to save your changes.

## Configuring Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service that will allow you to register your domain to their IP address, and will forward traffic directed at your domain to your frequently-changing IP address.

The router contains a client that can connect to a dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the router, whenever your ISP-assigned IP address changes, your router will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

## How to Configure Dynamic DNS

| | |
|---|---|
| | **Warning:** If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the dynamic DNS service will not work because private addresses will not be routed on the Internet. |

1. Log in to the router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, select **Dynamic DNS** to display the page below.

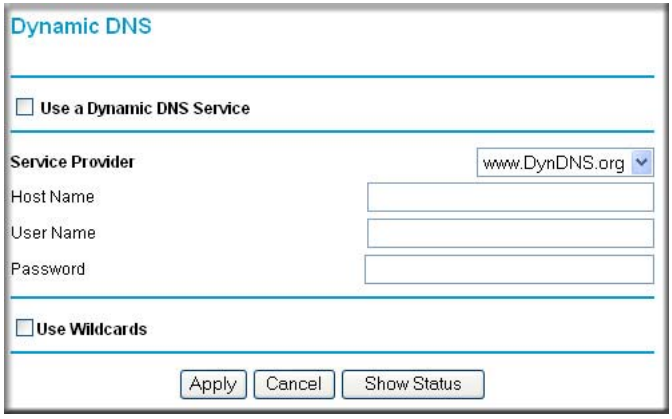



**Figure 7-4**

3. Access the Web site of one of the dynamic DNS service providers whose names appear in the ‘Service Provider’ box, and register for an account.
   For example, for dyndns.org, go to www.dyndns.org.
4. Select the **Use a dynamic DNS service** check box.
5. Select the name of your dynamic DNS Service Provider.

6. Type the Host Name that your dynamic DNS service provider gave you.
   The dynamic DNS service provider may call this the domain name. If your URL is myName.dyndns.org, then your Host Name is “myName.”
7. Type the User Name for your dynamic DNS account.
8. Type the Password (or key) for your dynamic DNS account.
9. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature.
   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
10. Click **Apply** to save your configuration.

# Using Static Routes

Static Routes provide additional routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

## Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router’s address on your LAN is 10.1.1.100.
- Your company’s network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the modem router, and a second static route was created to your local network for all 10.1.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company’s firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 10.1.1.100. The static route would look like Figure 7-5.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Modem Router IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 10.1.1.100.
- A Metric value of 1 will work since the ISDN router is on the LAN.
  This represents the number of routers between your network and the destination. This is a direct connection so it is set to 1.
- Private is selected only as a precautionary security measure in case RIP is activated.

## How to Configure Static Routes

1. Log in to the router at its default LAN address of http://10.1.1.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, click **Static Routes** to view the Static Routes menu.
3. To add or edit a Static Route:
   a. Click the **Edit** button to open the Edit Menu, shown in Figure 7-5.

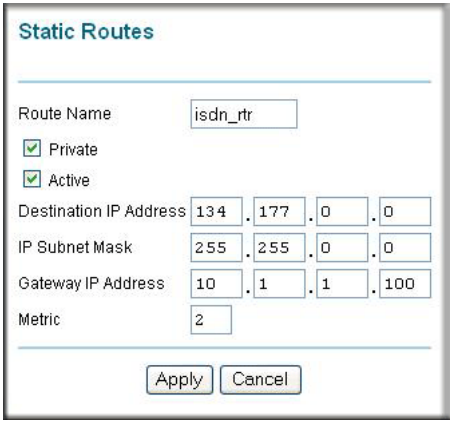



**Figure 7-5**

   b. Type a route name for this static route in the Route Name box under the table.
   This is for identification purposes only.

**c.** Select **Private** if you want to limit access to the LAN only.
The static route will not be reported in RIP.

**d.** Select **Active** to make this route effective.

**e.** Type the Destination IP Address of the final destination.

**f.** Type the IP Subnet Mask for this destination.
If the destination is a single host, type 255.255.255.255.

**g.** Type the Gateway IP Address, which must be a router on the same LAN segment as your DG834GSP ADSL Modem Wireless Router.

**h.** Type a number between 2 and 15 as the Metric value.
This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 2.

**4.** Click **Apply** to have the static route entered into the table.

**Figure 7-6**

# Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

1. Click **UPnP** on the main menu to invoke the UPnP menu:

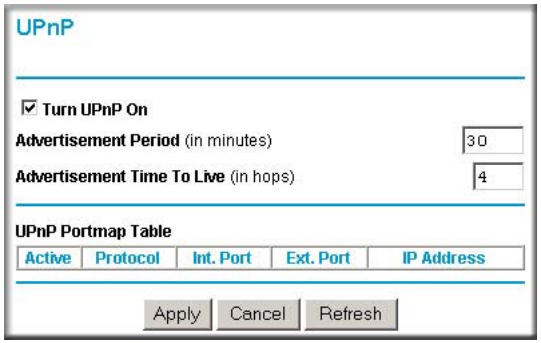



**Figure 7-7**

2. Fill out the UPnP screen:

   - **Turn UPnP On**: UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the Router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the Router.
   - **Advertisement Period**: The Advertisement Period is how often the Router will advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time To Live**: The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.
   - **UPnP Portmap Table**: The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the Router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

3. To save, cancel or refresh the table:

   **a.** Click **Apply** to save the new settings to the Router.

   **b.** Click **Cancel** to disregard any unsaved changes.

**c.** Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

# Chapter 8
# Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the ADSL Modem Wireless Router. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer. See "Virtual Private Networking (VPN)" in Appendix C to learn more about VPN.

This chapter is organized as follows:

- "Overview of VPN Configuration" on page 8-2 provides an overview of the two most common VPN configurations: Client-to-Gateway and Gateway-to-Gateway.
- "Planning a VPN" on page 8-4 provides a worksheet for recording the configuration parameters of the VPN you want to set up, along with the VPN Committee (VPNC) recommended default parameters set by the VPN Wizard.
- "VPN Tunnel Configuration" on page 8-6 summarizes the three ways to configure a VPN tunnel: VPN Wizard (recommended for most situations), Auto Policy, and Manual Policy.
- "How to Set Up a Client-to-Gateway VPN Configuration" on page 8-7 provides the steps needed to configure a VPN tunnel between a remote PC and a network gateway using the VPN Wizard and the NETGEAR ProSafe VPN Client.
- "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 8-21 provides the steps needed to configure a VPN tunnel between two network gateways using the VPN Wizard.
- "VPN Tunnel Control" on page 8-29 provides the step-by-step procedures for activating, verifying, deactivating, and deleting a VPN tunnel once the VPN tunnel has been configured.
- "How to Set Up VPN Tunnels in Special Circumstances" on page 8-38 provides the steps needed to configure VPN tunnels when there are special circumstances and the VPNC recommended defaults of the VPN Wizard are inappropriate. The two alternatives for configuring VPN tunnels are Auto Policy and Manual Policy.

# Overview of VPN Configuration

Two common scenarios for configuring VPN tunnels are between a remote personal computer and a network gateway and between two or more network gateways. The DG834GSP supports both of these types of VPN configurations. The ADSL Modem Wireless Router supports up to five concurrent tunnels.

## Client-to-Gateway VPN Tunnels

Client-to-Gateway VPN Tunnels provide secure access from a remote PC, such as a telecommuter connecting to an office network.

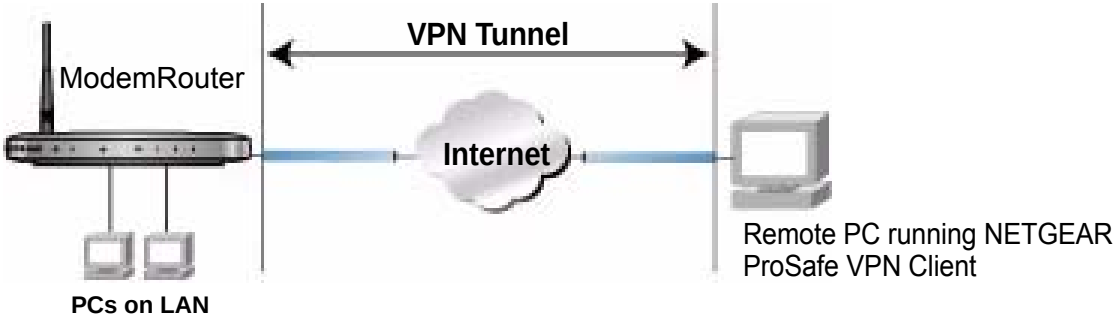



**Figure 8-1**

A VPN client access allows a remote PC to connect to your network from any location on the Internet. In this case, the remote PC is one tunnel endpoint, running the VPN client software. The ADSL Modem Wireless Router on your network is the other tunnel endpoint. See "How to Set Up a Client-to-Gateway VPN Configuration" on page 8-7 to set up this configuration.

## Gateway-to-Gateway VPN Tunnels

- Gateway-to-Gateway VPN Tunnels provide secure access between networks, such as a branch or home office and a main office.

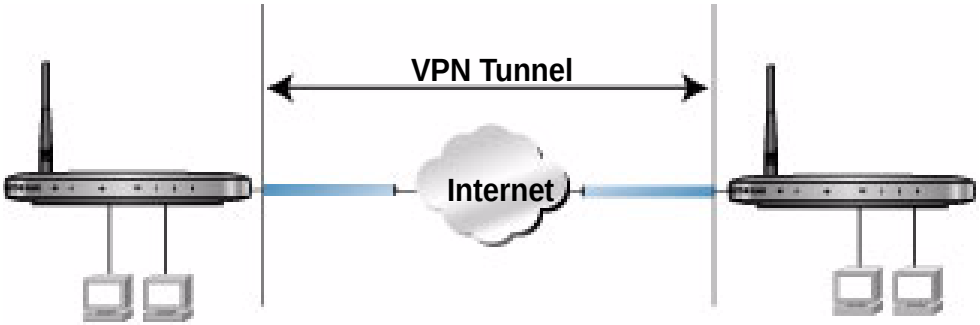



**Figure 8-2**

A VPN between two or more NETGEAR VPN-enabled modem routers is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use DG834GSPs on each end of the tunnel to form the VPN tunnel end points. See "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 8-21 to set up this configuration.

# Planning a VPN

When you set up a VPN, it is helpful to plan the network configuration and record the configuration parameters on a worksheet:

**Table 8-1. VPN Tunnel Configuration Worksheet**

| | |
|---|---|
| Connection Name: | |
| Pre-Shared Key: | |
| Secure Association -- Main Mode or Manual Keys: | |
| Perfect Forward Secrecy -- Enabled or Disabled: | |
| Encryption Protocol -- DES or 3DES: | |
| Authentication Protocol -- MD5 or SHA-1: | |
| Diffie-Hellman (DH) Group -- Group 1 or Group 2: | |
| Key Life in seconds: | |
| IKE Life Time in seconds: | |

| VPN Endpoint | Local IPSec ID | LAN IP Address | Subnet Mask | FQDN or Gateway IP (WAN IP Address) |
|---|---|---|---|---|
| | | | | |
| | | | | |

To set up a VPN connection, you must configure each endpoint with specific identification and connection information describing the other endpoint. You must configure the outbound VPN settings on one end to match the inbound VPN settings on other end, and vice versa.

This set of configuration information defines a security association (SA) between the two VPN endpoints. When planning your VPN, you must make a few choices first:

- Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single PC?

- Will either endpoint use Fully Qualified Domain Names (FQDNs)? FQDNs supplied by Dynamic DNS providers (see "The Use of a Fully Qualified Domain Name (FQDN)" on page B-8) can allow a VPN endpoint with a dynamic IP address to initiate or respond to a tunnel request. Otherwise, the side using a dynamic IP address must always be the initiator.
- What method will you use to configure your VPN tunnels?
  - The VPN Wizard using VPNC defaults (see Table 8-2)
  - The typical automated Internet Key Exchange (IKE) setup (see "Using Auto Policy to Configure VPN Tunnels" on page 8-38)
  - A Manual Keying setup in which you must specify each phase of the connection (see "Using Manual Policy to Configure VPN Tunnels" on page 8-48)?

**Table 8-2. Parameters Recommended by the VPNC and Used in the VPN Wizard**

| Parameter | Factory Default |
|---|---|
| Secure Association | Main Mode |
| Authentication Method | Pre-shared Key |
| Encryption Method | 3DES |
| Authentication Protocol | SHA-1 |
| Diffie-Hellman (DH) Group | Group 2 (1024 bit) |
| Key Life | 8 hours |
| IKE Life Time | 1 hour |

- What level of IPSec VPN encryption will you use?
  - DES - The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
  - 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- What level of authentication will you use?
  - MDS: 128 bits, faster but less secure.
  - SHA-1: 160 bits, slower but more secure.

# VPN Tunnel Configuration

There are two tunnel configurations and three ways to configure them:

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
  - — See "How to Set Up a Client-to-Gateway VPN Configuration" on page 8-7.
  - — See "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 8-21.
- See "Using Auto Policy to Configure VPN Tunnels" on page 8-38 when the VPN Wizard and its VPNC defaults (see Table 8-2) are not appropriate for your special circumstances, but you want to automate the Internet Key Exchange (IKE) setup.
- See "Using Manual Policy to Configure VPN Tunnels" on page 8-48 when the VPN Wizard and its VPNC defaults (see Table 8-2) are not appropriate for your special circumstances and you must specify each phase of the connection. You manually enter all the authentication and key parameters. You have more control over the process, however the process is more complex and there are more opportunities for errors or configuration mismatches between your DG834GSP and the corresponding VPN endpoint gateway or client workstation.

**Note:** NETGEAR publishes additional interoperability scenarios with various gateway and client software products. Look on the NETGEAR web site at *www.netgear.com* for these interoperability scenarios.

# How to Set Up a Client-to-Gateway VPN Configuration

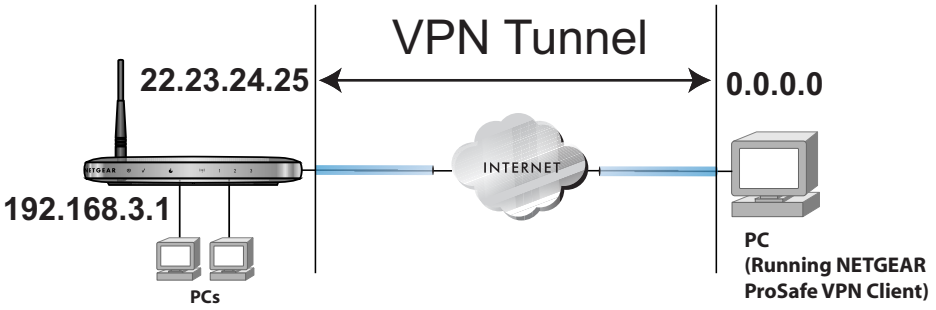



**Figure 8-3**

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway involves the following two steps:

- "Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834GSP" on page 8-7 uses the VPN Wizard to configure the VPN tunnel between the remote PC and network gateway.
- "Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC" on page 8-12 configures the NETGEAR ProSafe VPN Client endpoint.

## Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834GSP

| | |
|---|---|
| | **Note:** This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in Table 8-2 on page 8-5. If you have special requirements not covered by these VPNC-recommended parameters, refer to "How to Set Up VPN Tunnels in Special Circumstances" on page 8-38 to set up the VPN tunnel. |

The worksheet below identifies the parameters used in the following procedure. A blank worksheet is at "Planning a VPN" on page 8-4.

**Table 8-3. VPN Tunnel Configuration Worksheet**

| | |
|---|---|
| Connection Name: | **RoadWarrior** |
| Pre-Shared Key: | **12345678** |
| Secure Association -- Main Mode or Manual Keys: | **Main** |
| Perfect Forward Secrecy -- Enabled or Disabled: | **Disabled** |
| Encryption Protocol -- DES or 3DES: | **3DES** |
| Authentication Protocol -- MD5 or SHA-1: | **SHA-1** |
| Diffie-Hellman (DH) Group -- Group 1 or Group 2: | **Group 2** |
| Key Life in seconds: | **28800 (8 hours)** |
| IKE Life Time in seconds: | **3600 (1 hour)** |

| VPN Endpoint | Local IPSec ID | LAN IP Address | Subnet Mask | FQDN or Gateway IP (WAN IP Address) |
|---|---|---|---|---|
| **Client** | **to DG834GSP** | **—** | **—** | **Dynamic** |
| **DG834GSP** | **toClient** | **10.1.3.1** | **255.255.255.0** | **22.23.24.25** |

Follow this procedure to configure a client-to-gateway VPN tunnel using the VPN Wizard.

1. Log in to the DG834GSP at its LAN address of http://10.1.1.1 with its default user name of **admin** and password of **password**. Click the **VPN Wizard** link in the main menu to display this screen. Click **Next** to proceed.

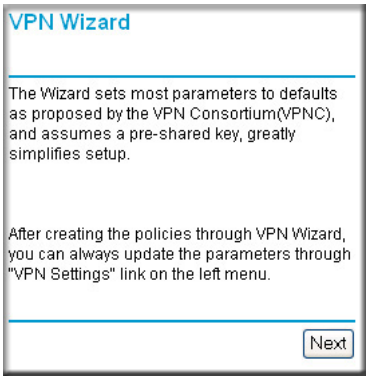

VPN Wizard
The Wizard sets most parameters to defaults as proposed by the VPN Consortium(VPNC), and assumes a pre-shared key, greatly simplifies setup.
After creating the policies through VPN Wizard, you can always update the parameters through "VPN Settings" link on the left menu.
Next

**Figure 8-4**

2. Fill in the Connection Name and the pre-shared key, select the type of target end point, and click **Next** to proceed.

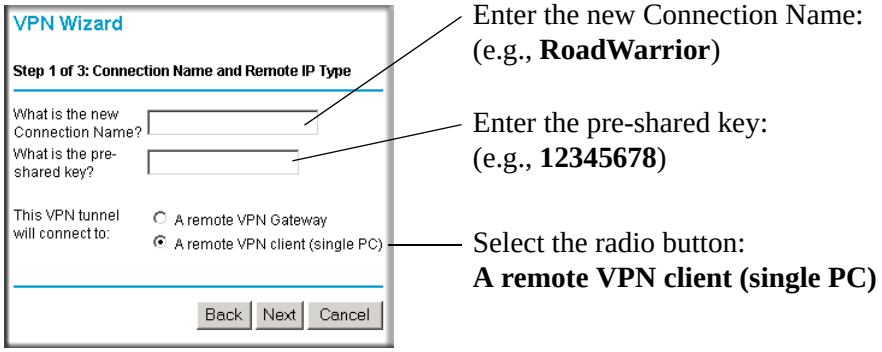

VPN Wizard
Step 1 of 3: Connection Name and Remote IP Type
What is the new Connection Name?
What is the pre-shared key?
This VPN tunnel will connect to:
A remote VPN Gateway
A remote VPN client (single PC)
Back
Next
Cancel
Enter the new Connection Name:
(e.g., RoadWarrior)
Enter the pre-shared key:
(e.g., 12345678)
Select the radio button:
A remote VPN client (single PC)

**Figure 8-5**

| | |
|---|---|
| | **Tip:** The Connection Name is arbitrary and not relevant to how the configuration functions. |

The Summary screen below displays.

**Figure 8-6**

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the "**here**" link. Click **Back** to return to the Summary screen.

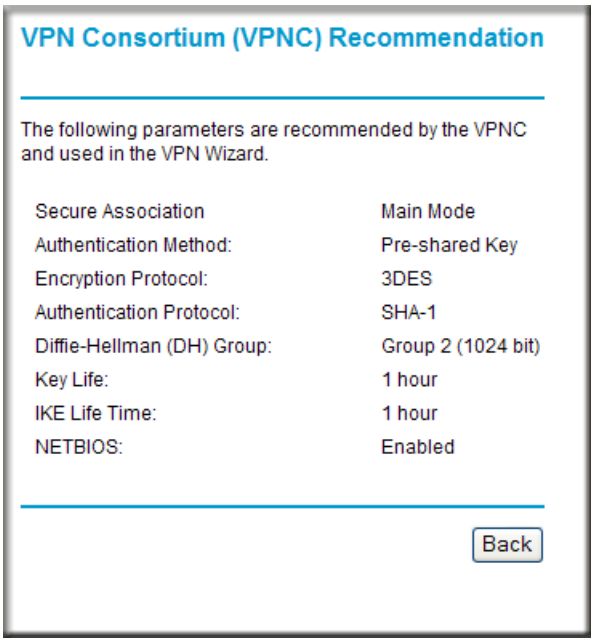



**Figure 8-7**

3. Click **Done** on the Summary screen to complete the configuration procedure. The VPN Policies menu below displays showing that the new tunnel is enabled.

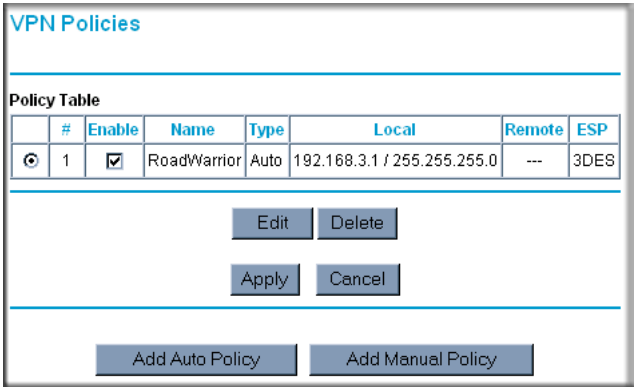



**Figure 8-8**

To view or modify the tunnel settings, select the radio button next to the tunnel entry and click **Edit**.

**Note:** Refer to "Using Auto Policy to Configure VPN Tunnels" on page 8-38 to enable the IKE keepalive capability on an existing VPN tunnel.

## Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC

This procedure describes how to configure the NETGEAR ProSafe VPN Client. We will assume the PC running the client has a dynamically assigned IP address.

The PC must have the NETGEAR ProSafe VPN Client program installed that supports IPSec. Go to the NETGEAR website (*http://www.netgear.com*) and select **VPN01L_VPN05L** in the Product Quick Find drop-down menu for information on how to purchase the NETGEAR ProSafe VPN Client.

**Note:** Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

1. Install the NETGEAR ProSafe VPN Client on the remote PC and reboot.
   - You may need to insert your Windows CD to complete the installation.
   - If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating "The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed." You can disregard this message.
   - Install the IPSec Component. You may have the option to install either the VPN Adapter or the IPSec Component or both. The VPN Adapter is not necessary.
   - The system should show the ProSafe icon ( ) in the system tray after rebooting.
   - Double-click the system tray icon to open the Security Policy Editor.
2. Add a new connection.
   a. Run the NETGEAR ProSafe Security Policy Editor program and, using the "VPN Tunnel Configuration Worksheet" on page 8-8, create a VPN Connection.

**b.** From the Edit menu of the Security Policy Editor, click **Add**, then **Connection**.

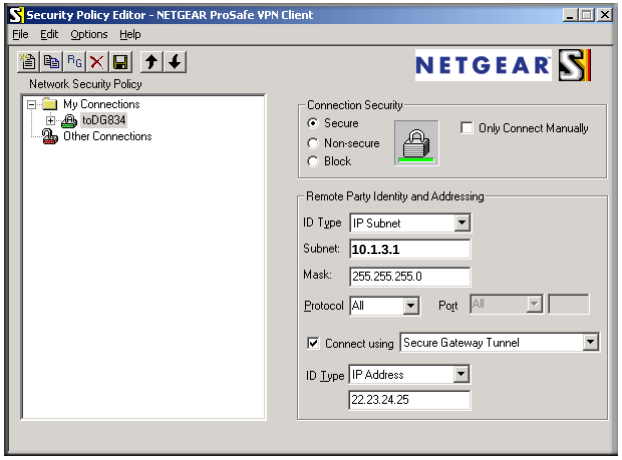



**Figure 8-9**

A “New Connection” listing appears in the list of policies. Rename the “New Connection” so that it matches the Connection Name you entered in the VPN Settings of the DG834GSP on LAN A.

| | |
|---|---|
| | **Note:** In this example, the Connection Name used on the client side of the VPN tunnel is **toDG834** and it does not have to match the **RoadWarrior** Connection Name used on the gateway side of the VPN tunnel because Connection Names are arbitrary to how the VPN tunnel functions. |

| | |
|---|---|
| | **Tip:** Choose Connection Names that make sense to the people using and administering the VPN. |

**c.** Select **Secure** in the Connection Security check-box group.

**d.** Select **IP Subnet** in the ID Type menu.

**e.** In this example, type **10.1.3.1** in the Subnet field as the network address of the DG834GSP.

**f.** Enter **255.255.255.0** in the Mask field as the LAN Subnet Mask of the DG834GSP.

**g.** Select **All** in the Protocol menu to allow all traffic through the VPN tunnel.

**h.** Select the **Connect using Secure Gateway Tunnel** check box.

**i.** Select **IP Address** in the ID Type menu below the check box.

**j.** Enter the public WAN IP Address of the DG834GSP in the field directly below the ID Type menu. In this example, **22.23.24.25** would be used.

**k.** The resulting Connection Settings are shown in Figure 8-10.

**3.** Configure the Security Policy in the NETGEAR ProSafe VPN Client software:

**a.** In the Network Security Policy list, expand the new connection by double clicking its name or clicking on the "+" symbol. My Identity and Security Policy subheadings appear below the connection name.

**b.** Click on the **Security Policy** subheading to show the Security Policy menu.

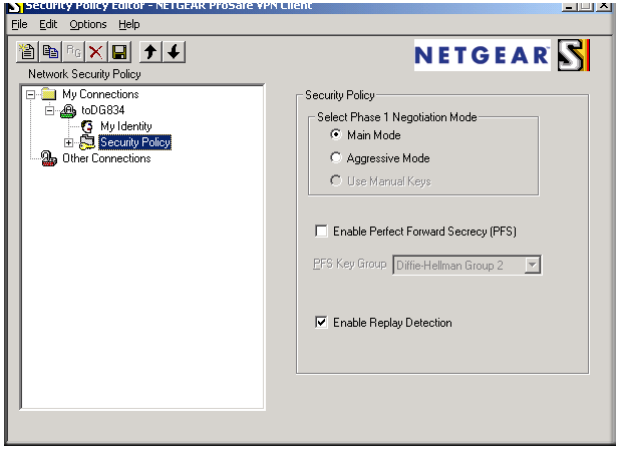



**Figure 8-10**

**c.** Select the **Main Mode** in the Select Phase 1 Negotiation Mode check-box group.

**4.** Configure the VPN Client Identity.

In this step, you will provide information about the remote VPN client PC. You will need to provide the Pre-Shared Key that you configured in the DG834GSP and either a fixed IP address or a "fixed virtual" IP address of the VPN client PC.

**a.** In the Network Security Policy list on the left side of the Security Policy Editor window, click on **My Identity**.

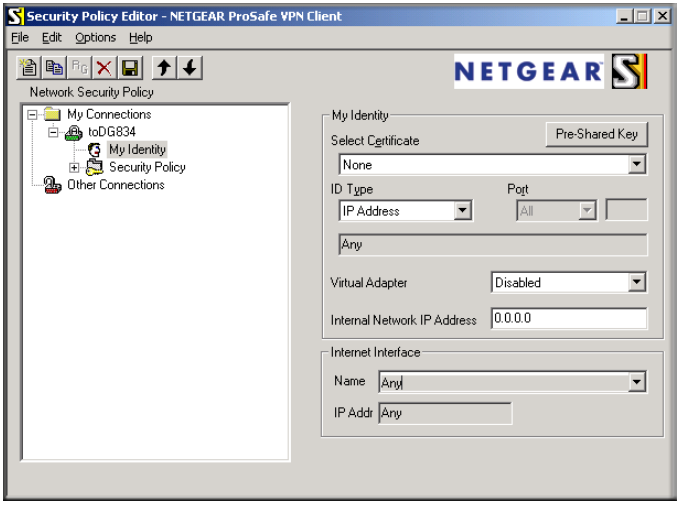



**Figure 8-11**

**b.** Choose **None** in the Select Certificate menu.

**c.** Select **IP Address** in the ID Type menu. If you are using a virtual fixed IP address, enter this address in the Internal Network IP Address box. Otherwise, leave this box empty.

**d.** In the Internet Interface box, select the adapter you use to access the Internet. Select **PPP Adapter** in the Name menu if you have a dial-up Internet account. Select your Ethernet adapter if you have a dedicated Cable or DSL line. You may also choose Any if you will be switching between adapters or if you have only one adapter.

**e.** Click the **Pre-Shared Key** button. In the Pre-Shared Key dialog box, click the **Enter** Key button. Enter the DG834GSP's Pre-Shared Key and click **OK**. In this example, **12345678** is entered. This field is case sensitive.

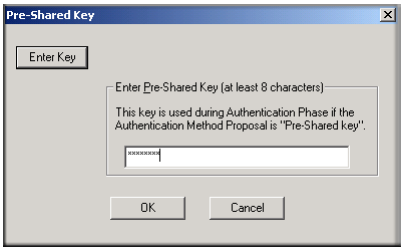

Pre-Shared Key
Enter Key
Enter Pre-Shared Key (at least 8 characters)
This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".
OK
Cancel

**Figure 8-12**

**5.** Configure the VPN Client Authentication Proposal.

In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the DG834GSP configuration.

**a.** In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double clicking its name or clicking on the "+" symbol.

**b.** Expand the Authentication subheading by double clicking its name or clicking on the "+" symbol. Then select **Proposal 1** below Authentication.

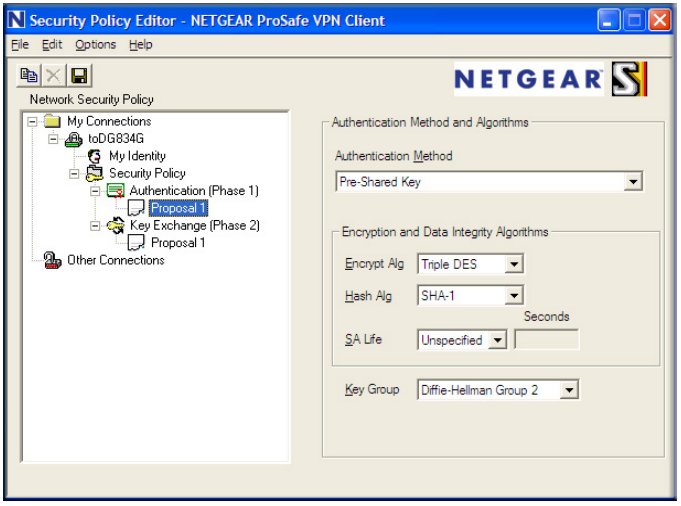



**Figure 8-13**

**c.** In the Authentication Method menu, select **Pre-Shared key**.

**d.** In the Encrypt Alg menu, select the type of encryption to correspond with what was configured for the Encryption Protocol in the DG834GSP in Table 8-3 on page 8-8. In this example, use Triple DES.

**e.** In the Hash Alg menu, select **SHA-1**.

**f.** In the SA Life menu, select **Unspecified**.

**g.** In the Key Group menu, select **Diffie-Hellman Group 2**.

**6.** Configure the VPN Client Key Exchange Proposal.

In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the DG834GSP configuration.

**a.** Expand the Key Exchange subheading by double clicking its name or clicking on the "+" symbol. Then select **Proposal 1** below Key Exchange.

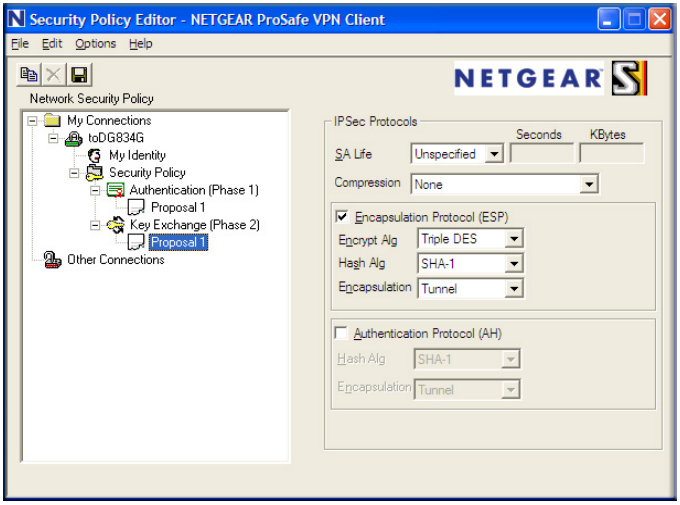



**Figure 8-14**

**b.** In the SA Life menu, select **Unspecified**.

**c.** In the Compression menu, select **None**.

**d.** Check the Encapsulation Protocol (ESP) checkbox.

**e.** In the Encrypt Alg menu, select the type of encryption to correspond with what was configured for the Encryption Protocol in the DG834GSP in Table 8-3 on page 8-8. In this example, use Triple DES.

**f.** In the Hash Alg menu, select **SHA-1**.

**g.** In the Encapsulation menu, select **Tunnel**.

**h.** Leave the Authentication Protocol (AH) checkbox unchecked.

**7.** Save the VPN Client Settings.

From the File menu at the top of the Security Policy Editor window, select **Save**.

After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router's LAN.

**8.** Check the VPN Connection.

To check the VPN Connection, you can initiate a request from the remote PC to the DG834GSP's network by using the "Connect" option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

To perform a ping test using our example, start from the remote PC:

**a.** Establish an Internet connection from the PC.

**b.** On the Windows taskbar, click the **Start** button, and then click **Run**.

**c.** Type **`ping -t 10.1.3.1`** , and then click **OK**.

This will cause a continuous ping to be sent to the first DG834GSP. After between several seconds and two minutes, the ping response should change from "timed out" to "reply."

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the remote DG834GSP. After a short wait, you should see the login screen of the Modem Router (unless another PC already has the DG834GSP management interface open).

Information on the progress and status of the VPN client connection can be viewed by opening the NETGEAR ProSafe Log Viewer.

To launch this function, click on the **Windows Start** button, then select **Programs**, then NETGEAR ProSafe VPN Client, then Log Viewer. The Log Viewer screen for a successful connection is shown below:

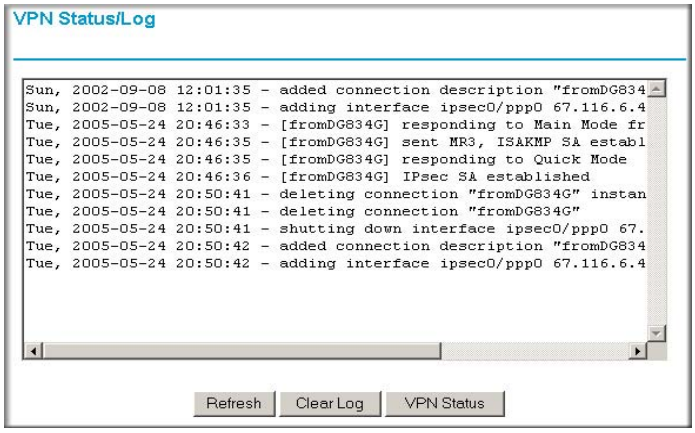

VPN Status/Log
Sun, 2002-09-08 12:01:35 - added connection description "fromDG834
Sun, 2002-09-08 12:01:35 - adding interface ipsec0/ppp0 67.116.6.4
Tue, 2005-05-24 20:46:33 - [fromDG834G] responding to Main Mode fr
Tue, 2005-05-24 20:46:35 - [fromDG834G] sent MR3, ISAKMP SA establ
Tue, 2005-05-24 20:46:35 - [fromDG834G] responding to Quick Mode
Tue, 2005-05-24 20:46:36 - [fromDG834G] IPsec SA established
Tue, 2005-05-24 20:50:41 - deleting connection "fromDG834G" instan
Tue, 2005-05-24 20:50:41 - deleting connection "fromDG834G"
Tue, 2005-05-24 20:50:41 - shutting down interface ipsec0/ppp0 67.
Tue, 2005-05-24 20:50:42 - added connection description "fromDG834
Tue, 2005-05-24 20:50:42 - adding interface ipsec0/ppp0 67.116.6.4
Refresh
Clear Log
VPN Status

**Figure 8-15**

| | |
|---|---|
| | **Note:** Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel. |

**9.** The Connection Monitor screen for this connection is shown below:

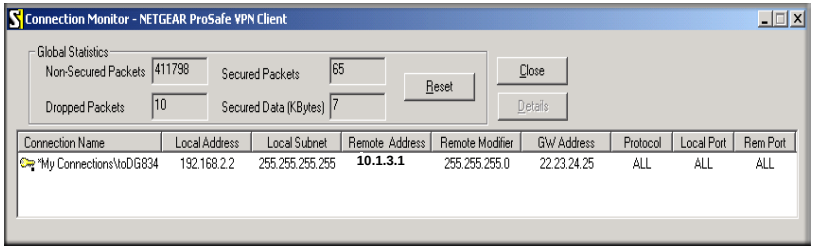



**Figure 8-16**

In this example you can see the following:

- The DG834GSP has a public IP WAN address of 22.23.24.25.
- The DG834GSP has a LAN IP address of 10.1.3.1.
- The VPN client PC has a dynamically assigned address of 10.1.2.2.

While the connection is being established, the Connection Name field in this menu will say “SA” before the name of the connection. When the connection is successful, the “SA” will change to the yellow key symbol shown in the illustration above.

| | |
|---|---|
| | **Note:** While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you will need to close the VPN connection in order to have normal Internet access. |

# How to Set Up a Gateway-to-Gateway VPN Configuration

**Note:** This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in Table 8-2 on page 8-5. If you have special requirements not covered by these VPNC-recommended parameters, refer to "How to Set Up VPN Tunnels in Special Circumstances" on page 8-38 to set up the VPN tunnel.

Follow this procedure to configure a gateway-to-gateway VPN tunnel using the VPN Wizard.

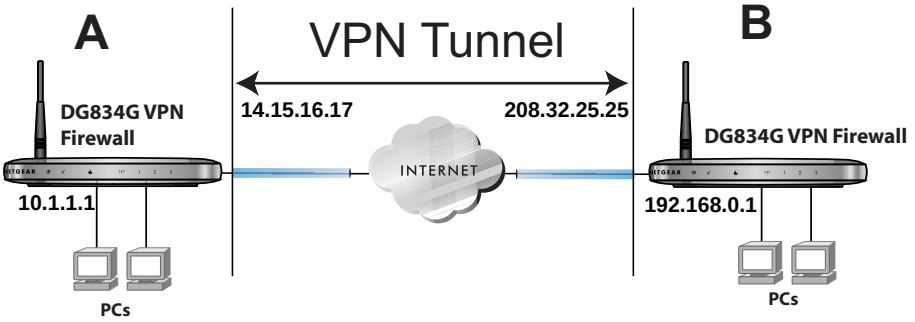



**Figure 8-17**

Set the LAN IPs on each DG834GSP to different subnets and configure each properly for the Internet. The examples below assume the following settings:

**Table 8-4. VPN Tunnel Configuration Worksheet**

| | |
|---|---|
| Connection Name: | **GtoG** |
| Pre-Shared Key: | **12345678** |
| Secure Association -- Main Mode or Manual Keys: | **Main** |
| Perfect Forward Secrecy -- Enabled or Disabled: | **Disabled** |
| Encryption Protocol -- DES or 3DES: | **3DES** |
| Authentication Protocol -- MD5 or SHA-1: | **SHA-1** |
| Diffie-Hellman (DH) Group -- Group 1 or Group 2: | **Group 2** |
| Key Life in seconds: | **28800 (8 hours)** |
| IKE Life Time in seconds: | **3600 (1 hour)** |

| VPN Endpoint | Local IPSec ID | LAN IP Address | Subnet Mask | FQDN or Gateway IP (WAN IP Address) |
|---|---|---|---|---|
| **DG834GSP_A** | **GW_A** | **10.1.1.1** | **255.255.255.0** | **14.15.16.17** |
| **DG834GSP_B** | **GW_B** | **192.168.0.1** | **255.255.255.0** | **208.32.25.25** |

**Note:** The LAN IP address ranges of each VPN endpoint must be different. The connection will fail if both are using the NETGEAR default address range of 10.1.1.x.

Follow this procedure to configure a gateway-to-gateway VPN tunnel using the VPN Wizard.

1. Log in to the DG834GSP on LAN A at its default LAN address of http://10.1.1.1 with its default user name of **admin** and password of **password**. Click the **VPN Wizard** link in the main menu to display this screen. Click **Next** to proceed.

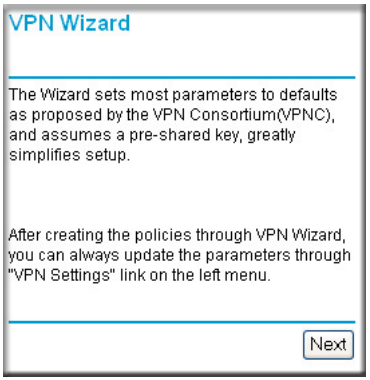

VPN Wizard
The Wizard sets most parameters to defaults as proposed by the VPN Consortium(VPNC), and assumes a pre-shared key, greatly simplifies setup.
After creating the policies through VPN Wizard, you can always update the parameters through "VPN Settings" link on the left menu.
Next

**Figure 8-18**

2. Fill in the Connection Name and the pre-shared key, select the type of target end point, and click **Next** to proceed.

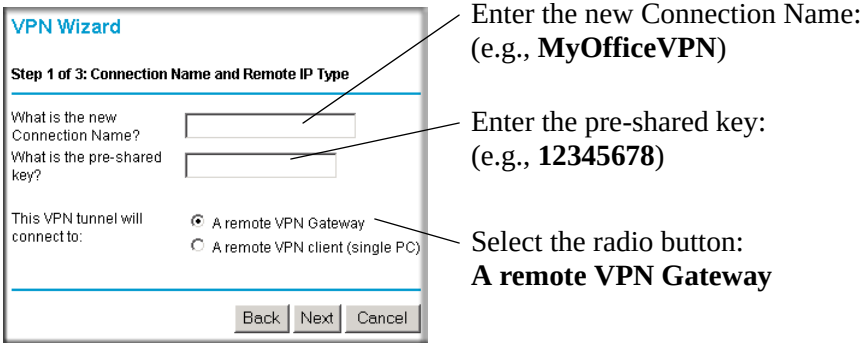
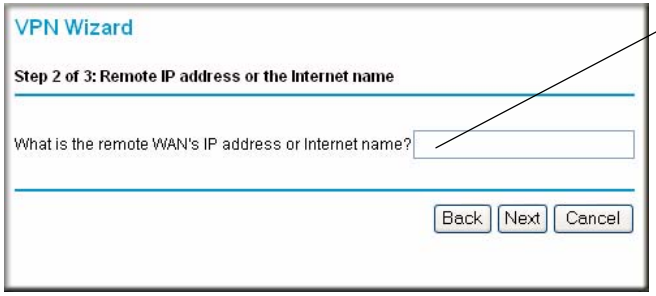



**Figure 8-19**

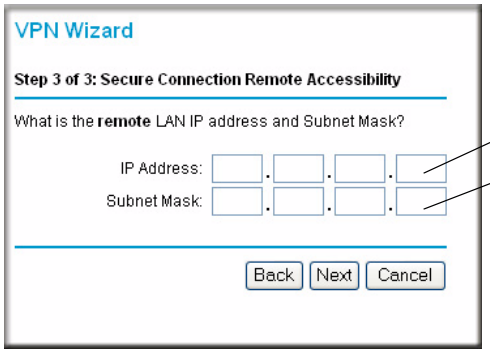
**3.** Fill in the IP Address or FQDN for the target VPN endpoint WAN connection and click **Next**.


VPN Wizard
Step 2 of 3: Remote IP address or the Internet name
What is the remote WAN's IP address or Internet name?
Back
Next
Cancel

Enter the WAN IP address of the remote VPN gateway: (e.g., **208.32.25.25**)

**Figure 8-20**

**4.** Identify the IP addresses at the target endpoint that can use this tunnel, and click **Next**.




Enter the LAN IP settings of the remote VPN gateway:

- IP Address (e.g., **10.1.1.1**)
- Subnet Mask (e.g., **255.255.255.0**)

**Figure 8-21**

The Summary screen below displays.

**Figure 8-22**

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the "**here**" link (see Figure 8-22). Click **Back** to return to the Summary screen.

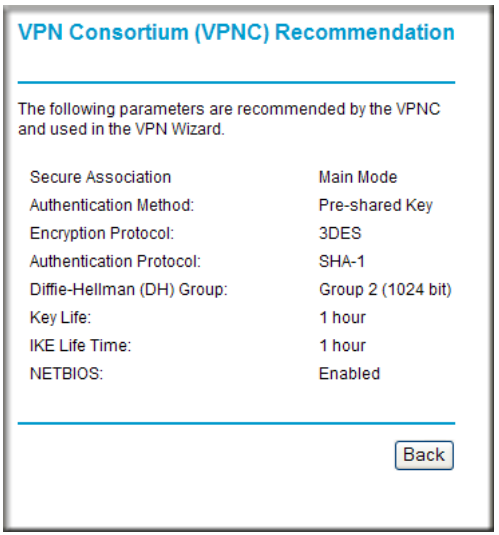



**Figure 8-23**

5. Click **Done** on the Summary screen (see Figure 8-22) to complete the configuration procedure. The VPN Settings menu below displays showing that the new tunnel is enabled.

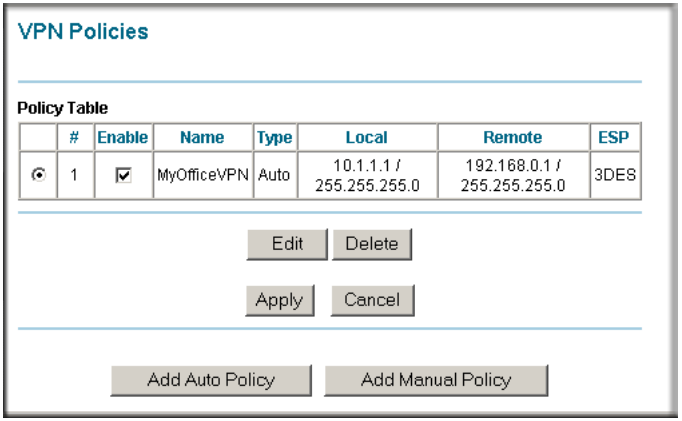



**Figure 8-24**

**Note:** Refer to "Using Auto Policy to Configure VPN Tunnels" on page 8-38 to enable the IKE keep-alive capability on an existing VPN tunnel.

6. Repeat for the DG834GSP on LAN B and pay special attention to use the following network settings as appropriate.
   - WAN IP of the remote VPN gateway (e.g., **14.15.16.17**)
   - LAN IP settings of the remote VPN gateway:
     - IP Address (e.g, **10.1.1.1**)
     - Subnet Mask (e.g., **255.255.255.0**)
     - Preshared Key (e.g., **12345678**)
7. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

**Note:** The VPN Status screen is only one of three ways to active a VPN tunnel. See "Activating a VPN Tunnel" on page 8-29 for information on the other ways.

**a.** Open the DG834GSP management interface and click on **VPN Status** to get the VPN Status/Log screen (Figure 8-25).

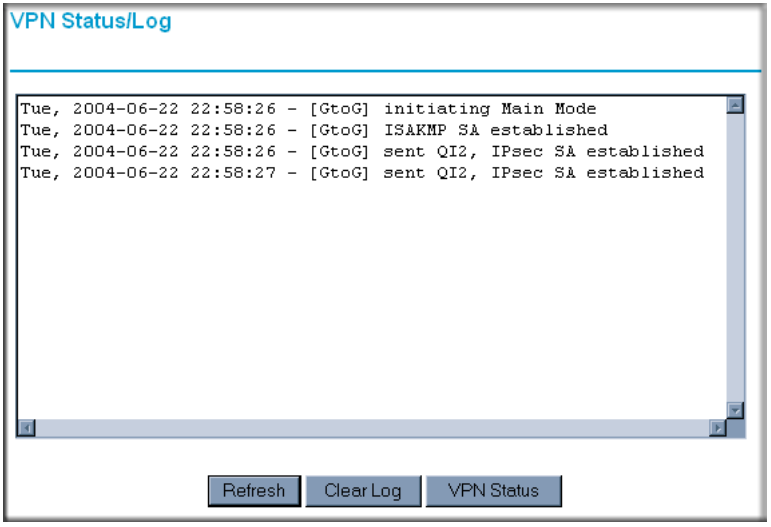

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

**Figure 8-25**

**b.** Click on **VPN Status** (Figure 8-27) to get the Current VPN Tunnels (SAs) screen (Figure 8-26). Click on **Connect** for the VPN tunnel you want to activate.

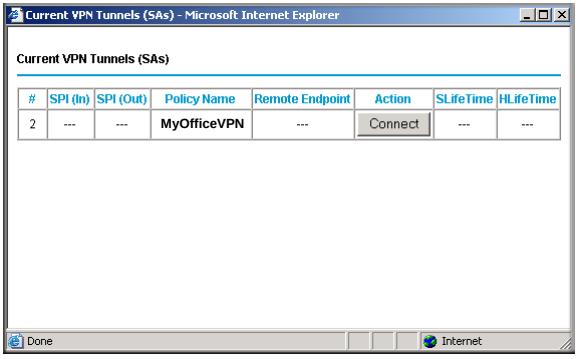

Current VPN Tunnels (SAs) - Microsoft Internet Explorer
Current VPN Tunnels (SAs)
# SPI (In) SPI (Out) Policy Name Remote Endpoint Action SLifeTime HLifeTime
2 --- --- MyOfficeVPN --- Connect --- ---
Done
Internet

**Figure 8-26**

**c.** Look at the VPN Status/Log screen (Figure 8-25) to verify that the tunnel is connected.

# VPN Tunnel Control

## Activating a VPN Tunnel

There are three ways to activate a VPN tunnel:

- Use the VPN Status page.
- Activate the VPN tunnel by pinging the remote endpoint.
- Start using the VPN tunnel.

**Note:** Refer to "Using Auto Policy to Configure VPN Tunnels" on page 8-38 to enable the IKE keepalive capability on an existing VPN tunnel.

### Using the VPN Status Page to Activate a VPN Tunnel

To use the VPN Status screen to activate a VPN tunnel, perform the following steps:

1. Log in to the Modem Router.
2. Open the DG834GSP management interface and click on **VPN Status** to get the VPN Status/ Log screen (Figure 8-27).

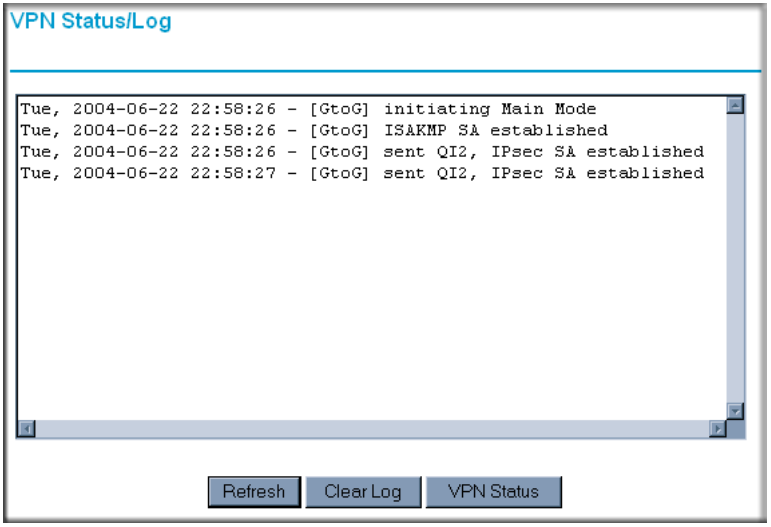

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

**Figure 8-27**

3. Click on **VPN Status** (Figure 8-27) to get the Current VPN Tunnels (SAs) screen (Figure 8-28). Click on **Connect** for the VPN tunnel you want to activate.

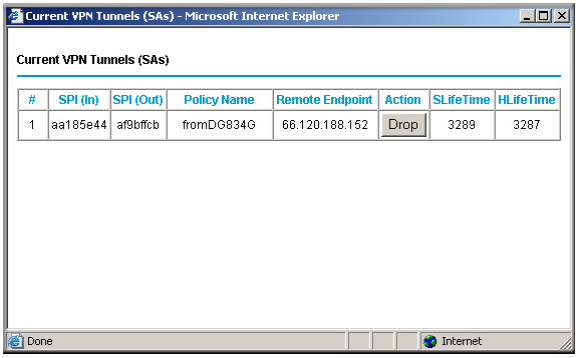

Current VPN Tunnels (SAs) - Microsoft Internet Explorer
Current VPN Tunnels (SAs)
# SPI (In) SPI (Out) Policy Name Remote Endpoint Action SLifeTime HLifeTime
1 aa185e44 af9bffcb fromDG834G 66.120.188.152 Drop 3289 3287
Done
Internet

**Figure 8-28**

## Activate the VPN Tunnel by Pinging the Remote Endpoint

**Note:** This section uses 10.1.3.1 for an example remote endpoint LAN IP address.

To activate the VPN tunnel by pinging the remote endpoint (e.g., 192.168.0.1), do the following steps depending on whether your configuration is client-to-gateway or gateway-to-gateway:

- **Client-to-Gateway Configuration**—to check the VPN Connection, you can initiate a request from the remote PC to the DG834GSP's network by using the "Connect" option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

  To perform a ping test using our example, start from the remote PC:

  **a.** Establish an Internet connection from the PC.

  **b.** On the Windows taskbar, click the **Start** button, and then click **Run**.

  **c.** Type `ping -t 192.168.0.1` and then click **OK**.

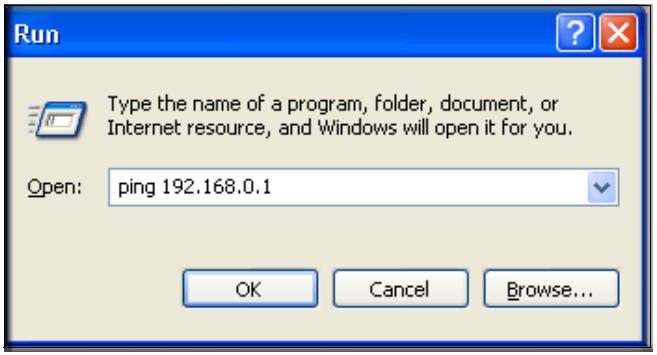



**Figure 8-29: Running a Ping test to the LAN from the PC**

This will cause a continuous ping to be sent to the first DG834GSP. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.”

| | |
|---|---|
| | **Note:** Use **Ctrl-C** to stop the pinging. |

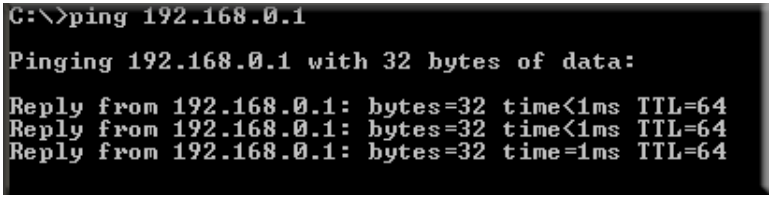

C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

**Figure 8-30**

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the remote DG834GSP. After a short wait, you should see the login screen of the Modem Router (unless another PC already has the DG834GSP management interface open).

- **Gateway-to-Gateway Configuration**—test the VPN tunnel by pinging the remote network from a PC attached to the DG834GSP.

  **a.** Open command prompt (i.e., Start -> Run -> cmd).

**b.** ping 10.1.1.1.

| | |
|---|---|
| | **Note:** The pings may fail the first time. If so, then try the pings a second time. |

### Start Using a VPN Tunnel to Activate It

To use a VPN tunnel, use a Web browser to go to a URL whose IP address or range is covered by the policy for that VPN tunnel.

## Verifying the Status of a VPN Tunnel

To use the VPN Status page to determine the status of a VPN tunnel, perform the following steps:

1. Log in to the Modem Router.
2. Open the DG834GSP management interface and click on **VPN Status** to get the VPN Status/ Log screen (Figure 8-31).

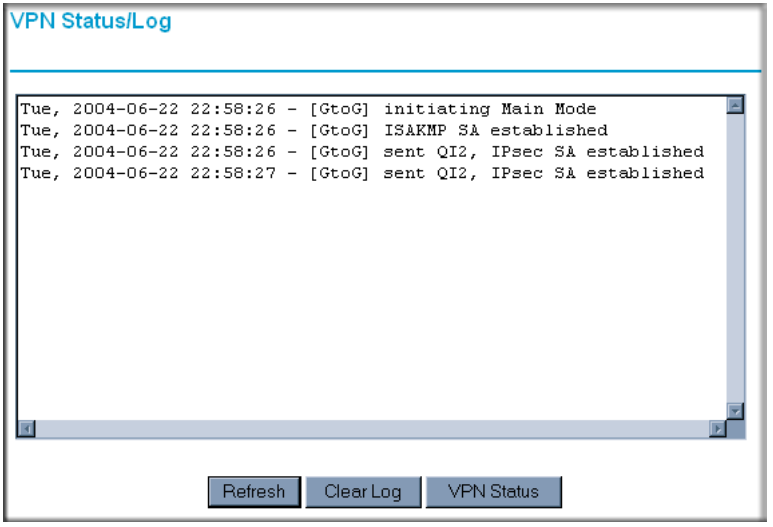

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

**Figure 8-31**

Log—this log shows the details of recent VPN activity, including the building of the VPN tunnel. If there is a problem with the VPN tunnel, refer to the log for information about what might be the cause of the problem.

- Click **Refresh** to see the most recent entries.
- Click **Clear Log** to delete all log entries.

3. Click on **VPN Status** (Figure 8-27) to get the Current VPN Tunnels (SAs) screen.

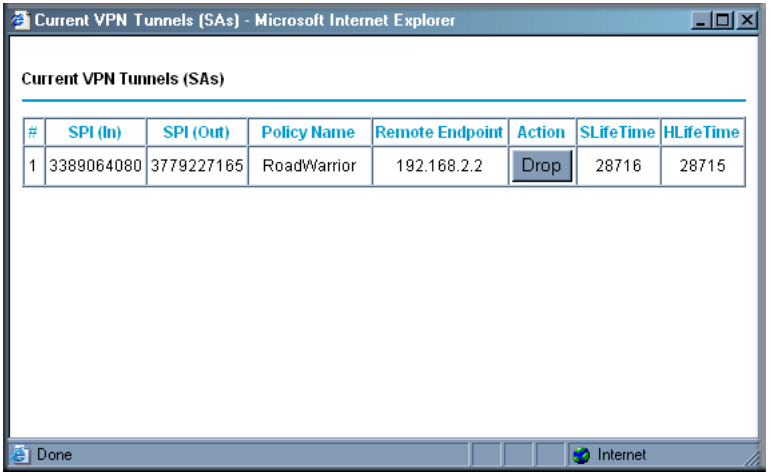

Current VPN Tunnels (SAs) - Microsoft Internet Explorer
Current VPN Tunnels (SAs)
# SPI (In) SPI (Out) Policy Name Remote Endpoint Action SLifeTime HLifeTime
1 3389064080 3779227165 RoadWarrior 192.168.2.2 Drop 28716 28715
Done
Internet

**Figure 8-32**

This table lists the following data for each active VPN Tunnel.

- **SPI**—each SA has a unique SPI (Security Parameter Index) for traffic in each direction. For "Manual" key exchange, the SPI is specified in the Policy definition. For "Automatic" key exchange, the SPI is generated by the IKE protocol.
- **Policy Name**—the name of the VPN policy associated with this SA.
- **Remote Endpoint**—the IP address on the remote VPN Endpoint.
- **Action**—the action will be either a "Drop" or a "Connect" button.
- **SLifeTime (Secs)**—the remaining Soft Lifetime for this SA in seconds. When the Soft Lifetime becomes zero, the SA (Security Association) will re-negotiated.
- **HLifeTime (Secs)**—the remaining Hard Lifetime for this SA in seconds. When the Hard Lifetime becomes zero, the SA (Security Association) will be terminated. (It will be re-established if required.)

## Deactivating a VPN Tunnel

Sometimes a VPN tunnel must be deactivated for testing purposes. There are two ways to deactivate a VPN tunnel:

- Policy table on VPN Policies page
- VPN Status page

### Using the Policy Table on the VPN Policies Page to Deactivate a VPN Tunnel

To use the VPN Policies page to deactivate a VPN tunnel, perform the following steps:

1. Log in to the Modem Router.
2. Open the DG834GSP management interface and click on **VPN Policies** to get the VPN Policies screen (Figure 8-33).

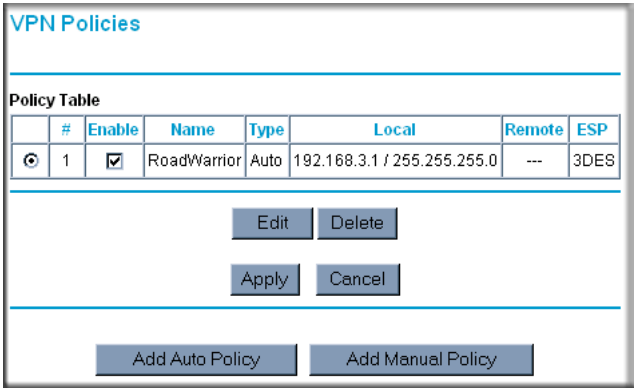



**Figure 8-33**

3. Clear the Enable check box for the VPN tunnel you want to deactivate and click **Apply**. (To reactivate the tunnel, check the Enable box and click **Apply**.)

### Using the VPN Status Page to Deactivate a VPN Tunnel

To use the VPN Status page to deactivate a VPN tunnel, perform the following steps:

1. Log in to the Modem Router.

2. Open the DG834GSP management interface and click on **VPN Status** to get the VPN Status/ Log screen (Figure 8-34).

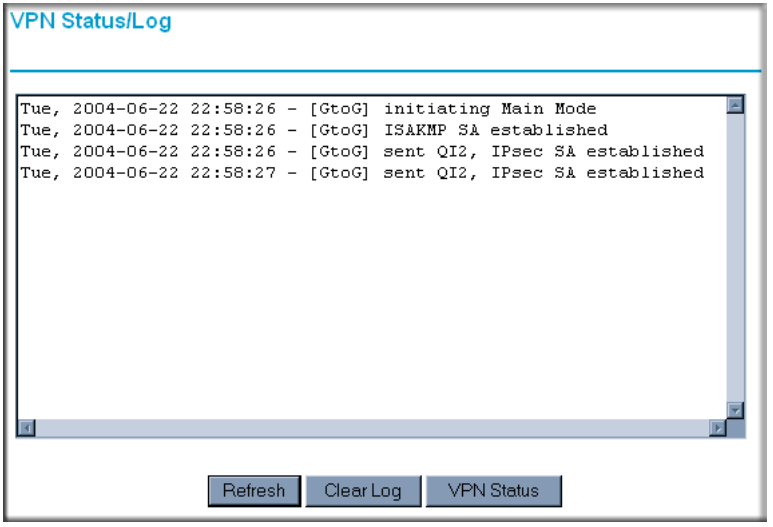

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

**Figure 8-34**

3. Click **VPN Status** (Figure 8-34) to get the Current VPN Tunnels (SAs) screen (Figure 8-35). Click **Drop** for the VPN tunnel you want to deactivate.

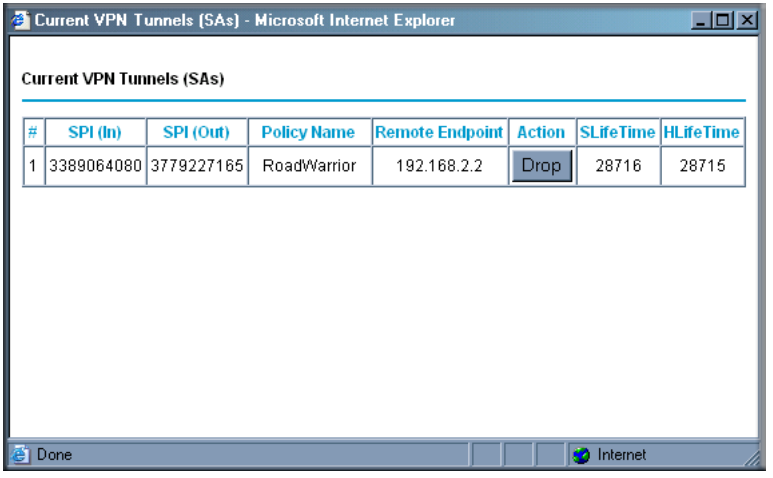

Current VPN Tunnels (SAs) - Microsoft Internet Explorer
Current VPN Tunnels (SAs)
# SPI (In) SPI (Out) Policy Name Remote Endpoint Action SLifeTime HLifeTime
1 3389064080 3779227165 RoadWarrior 192.168.2.2 Drop 28716 28715
Done
Internet

**Figure 8-35**

## Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the Modem Router.
2. Open the DG834GSP management interface and click **VPN Policies** to display the VPN Policies screen (Figure 8-36). Select the radio button for the VPN tunnel to be deleted and click the **Delete** button.

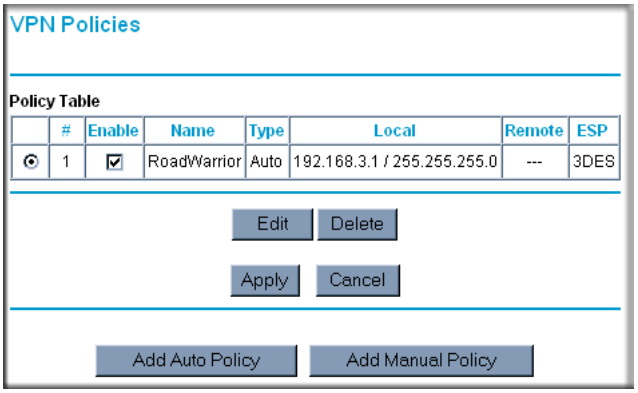



**Figure 8-36**

# How to Set Up VPN Tunnels in Special Circumstances

When the VPN Wizard and its VPNC defaults (see Table 8-2) are not appropriate for your special circumstances, use one of the following alternatives:

- **Auto Policy**—for a typical automated Internet Key Exchange (IKE) setup, see "Using Auto Policy to Configure VPN Tunnels" on page 8-38. Auto Policy uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys.
- **Manual Policy**—for a Manual Keying setup in which you must specify each phase of the connection, see "Using Manual Policy to Configure VPN Tunnels" on page 8-48. Manual Policy does not use IKE. Rather, you manually enter all the authentication and key parameters. You have more control over the process, however the process is more complex and there are more opportunities for errors or configuration mismatches between your DG834GSP and the corresponding VPN endpoint gateway or client workstation.

## Using Auto Policy to Configure VPN Tunnels

You need to configure matching VPN settings on both VPN endpoints. The outbound VPN settings on one end must match to the inbound VPN settings on other end, and vice versa.

See "Example of Using Auto Policy" on page 8-43 for an example of using Auto Policy.

### Configuring VPN Network Connection Parameters

All VPN tunnels on the ADSL Modem Wireless Router require configuring several network parameters. This section describes those parameters and how to access them.

The most common configuration scenarios will use IKE to manage the authentication and encryption keys. The IKE protocol performs negotiations between the two VPN endpoints to automatically generate and update the required encryption parameters.

Click the **VPN Policies** link of the main menu, and then click the **Add Auto Policy** button to display the VPN - Auto Policy menu shown in Figure 8-37.

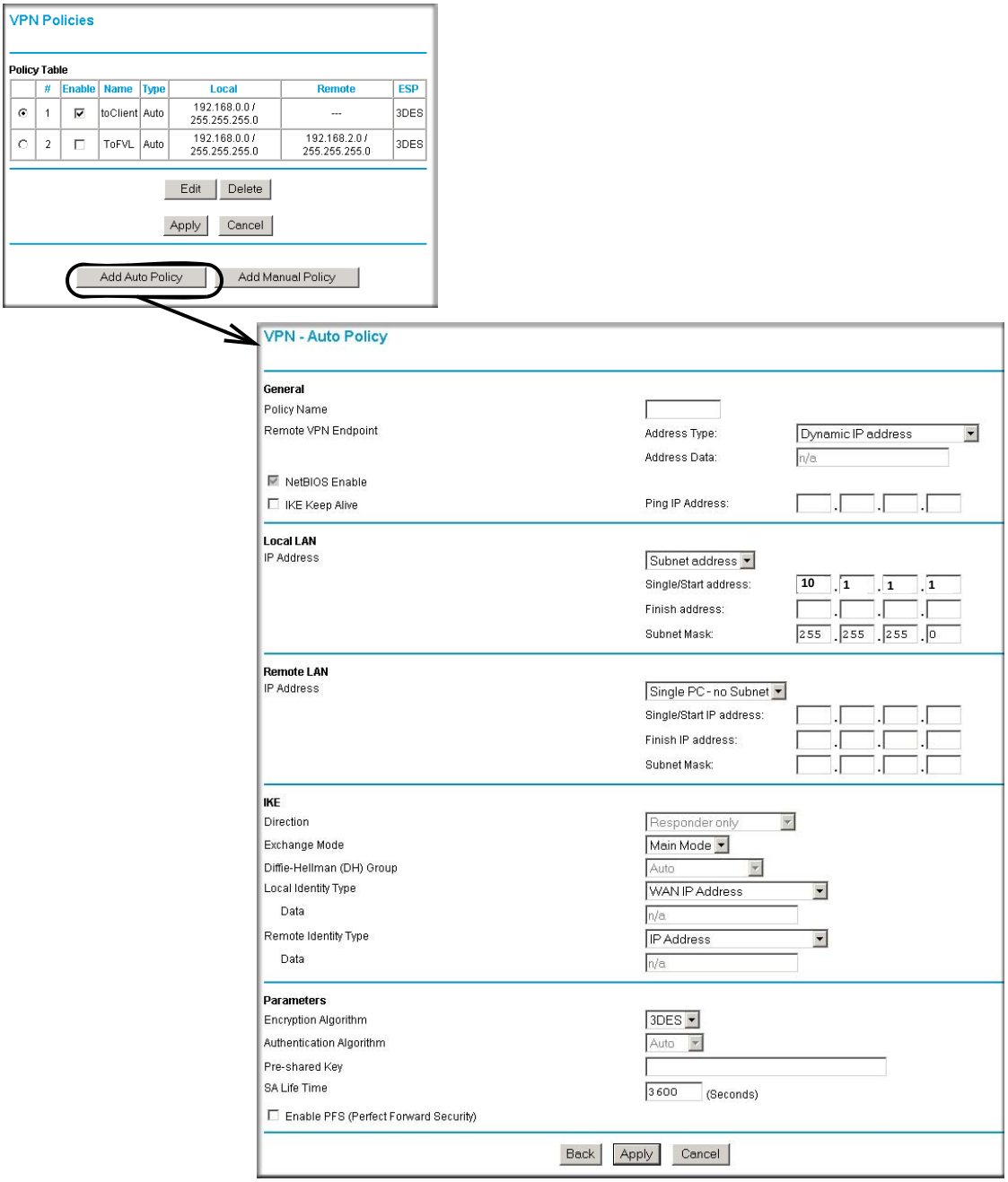

VPN Policies
Policy Table
# Enable Name Type Local Remote ESP
1 toClient Auto 192.168.0.0 / 255.255.255.0 --- 3DES
2 ToFVL Auto 192.168.0.0 / 255.255.255.0 192.168.2.0 / 255.255.255.0 3DES
Edit
Delete
Apply
Cancel
Add Auto Policy
Add Manual Policy
VPN - Auto Policy
General
Policy Name
Remote VPN Endpoint
Address Type:
Dynamic IP address
Address Data:
n/a
NetBIOS Enable
IKE Keep Alive
Ping IP Address:
Local LAN
IP Address
Subnet address
Single/Start address:
10 . 1 . 1 . 1
Finish address:
Subnet Mask:
255 . 255 . 255 . 0
Remote LAN
IP Address
Single PC - no Subnet
Single/Start IP address:
Finish IP address:
Subnet Mask:
IKE
Direction
Responder only
Exchange Mode
Main Mode
Diffie-Hellman (DH) Group
Auto
Local Identity Type
WAN IP Address
Data
n/a
Remote Identity Type
IP Address
Data
n/a
Parameters
Encryption Algorithm
3DES
Authentication Algorithm
Auto
Pre-shared Key
SA Life Time
3600
(Seconds)
Enable PFS (Perfect Forward Security)
Back
Apply
Cancel

**Figure 8-37**

The DG834GSP VPN tunnel network connection fields are defined as follows:

***General.*** These settings identify this policy and determine its major characteristics.

- **Policy Name**—Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**—If the remote endpoint has a dynamic IP address, select **Dynamic IP address**. No "Address Data" input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint to which you wish to connect.

**Note:** The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".

- **IKE Keep-alive**—Enable this if you wish to ensure that a connection is kept open, or, if that is not possible, that it is quickly re-established when disconnected.

  The Ping IP Address must be associated with the remote endpoint. The remote LAN address must be used. This IP address will be "pinged" periodically to generate traffic for the VPN tunnel. The remote keep-alive IP address must be covered by the remote LAN IP range and must correspond to a device that can respond to ping. The range should be made as narrow as possible to meet this objective.

***Local LAN.*** This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single address**—enter an IP address in the "Single/Start IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on your LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field. The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.
- **Any**—the remote VPN endpoint may be at any IP address.

***Remote LAN.*** This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single PC - no Subnet**—select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. The typical application is a PC running the VPN client at the remote end.
- **Single address**—Enter an IP address in the "Single/Start IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on the remote LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.
- **Any**—any outgoing traffic from the “Local IP” computers will trigger an attempted VPN connection to the remote VPN endpoint. Please be sure you want this option before selecting it.

The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.

***IKE.*** **Direction/Type**—this setting is used when determining if the IKE policy matches the current traffic. Select the desired option.

- **Responder only**—incoming connections are allowed, but outgoing connections will be blocked.
- **Initiator and Responder**—both incoming and outgoing connections are allowed.

**Exchange Mode**—ensure the remote VPN endpoint is set to use "Main Mode".

**Diffie-Hellman (DH) Group**—the Diffie-Hellman algorithm is used when exchanging keys. The DH Group setting determines the number of bit size used in the exchange. This value must match the value used on the remote VPN Gateway.

**Local Identity Type**—select the desired option to match the "Remote Identity Type" setting on the remote VPN endpoint.

- **WAN IP Address**—your Internet IP address.
- **Fully Qualified Domain Name**—your domain name.
- **Fully Qualified User Name**—your name, E-mail address, or other ID.

**Local Identity Data**—enter the data for the selection above. (If **WAN IP Address** is selected, no input is required.)

**Remote Identity Type**—select the desired option to match the "Local Identity Type" setting on the remote VPN endpoint.

- **IP Address**—the Internet IP address of the remote VPN endpoint.
- **Fully Qualified Domain Name**—the Domain name of the remote VPN endpoint.
- **Fully Qualified User Name**—the name, E-mail address, or other ID of the remote VPN endpoint.

**Remote Identity Data**—enter the data for the selection above. (If **IP Address** is selected, no input is required.)

***Parameters.*** **Encryption Algorithm**—encryption Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway. DES and 3DES are supported.

- DES—the Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
- 3DES—(Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

**Authentication Algorithm**—authentication Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway. Auto, MD5, and SHA-1 are supported. Auto negotiates with the remote VPN endpoint and is not available in responder-only mode.

- MD5—128 bits, faster but less secure.
- SHA-1 (default)—160 bits, slower but more secure.

**Pre-shared Key**—the key must be entered both here and on the remote VPN Gateway.

**SA Life Time**—this determines the time interval before the SA (Security Association) expires. (It will automatically be re-established as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA Life Time. This setting applies to both IKE and IPSec SAs.

**IPSec PFS (Perfect Forward Secrecy)**—if enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you may have to specify the "Key Group" used. For this device, the "Key Group" is the same as the "DH Group" setting in the IKE section.

### Example of Using Auto Policy

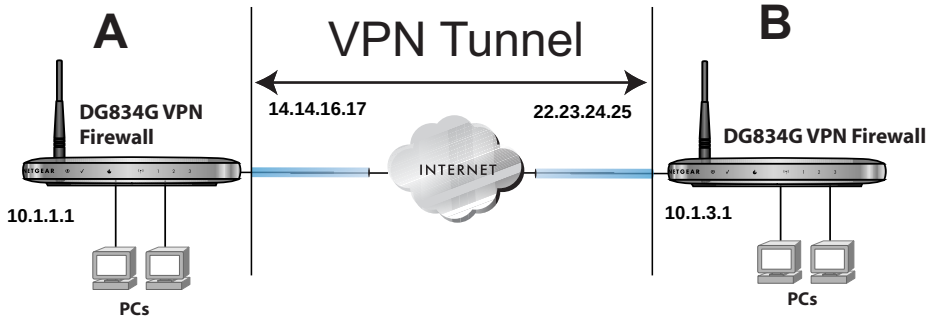



**Figure 8-38**

**1.** Set the LAN IPs on each DG834GSP to different subnets and configure each properly for the Internet. The following settings are assumed for this example:

**Table 8-5. VPN Tunnel Configuration Worksheet**

| | |
|---|---|
| Connection Name: | **GtoG** |
| Pre-Shared Key: | **12345678** |
| Secure Association -- Main Mode or Manual Keys: | **Main** |
| Perfect Forward Secrecy -- Enabled or Disabled: | **Disabled** |
| Encryption Protocol -- DES or 3DES: | **3DES** |
| Authentication Protocol -- MD5 or SHA-1: | **SHA-1** |
| Diffie-Hellman (DH) Group -- Group 1 or Group 2: | **Group 2** |
| Key Life in seconds: | **28800 (8 hours)** |
| IKE Life Time in seconds: | **3600 (1 hour)** |

| VPN Endpoint | Local IPSec ID | LAN IP Address | Subnet Mask | FQDN or Gateway IP (WAN IP Address) |
|---|---|---|---|---|
| **DG834GSP A** | **LAN_A** | **10.1.1.1** | **255.255.255.0** | **14.15.16.17** |
| **DG834GSP B** | **LAN_B** | **10.1.3.1** | **255.255.255.0** | **22.23.24.25** |

2. Open the DG834GSP on LAN A management interface and click on **VPN Policies**.

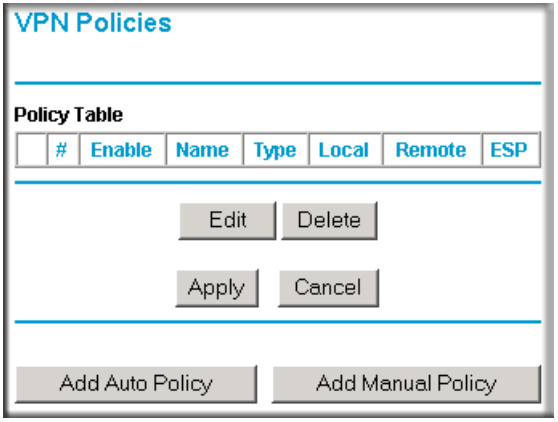



**Figure 8-39**

3. Click **Add Auto Policy**.
4. Enter policy settings (see Figure 8-40).
   - General
     - Policy Name = GtoG
     - Remote VPN Endpoint Address Type = Fixed IP Address
     - Remote VPN Endpoint Address Data = 22.23.24.25
   - Local LAN – use default setting
   - Remote LAN
     - IP Address = select Subnet address from the pulldown menu.
     - Start IP address = 10.1.3.1
     - Subnet Mask = 255.255.255.0
   - IKE
     - Direction = Initiator and Responder
     - Exchange Mode = Main Mode
     - Diffie-Hellman (DH) Group = Group 2 (1024 Bit)
     - Local Identity Type = use default setting
     - Remote Identity Type = use default setting
   - Parameters
     - Encryption Algorithm = 3DES

— Authentication Algorithm = MD5

— Pre-shared Key = 12345678

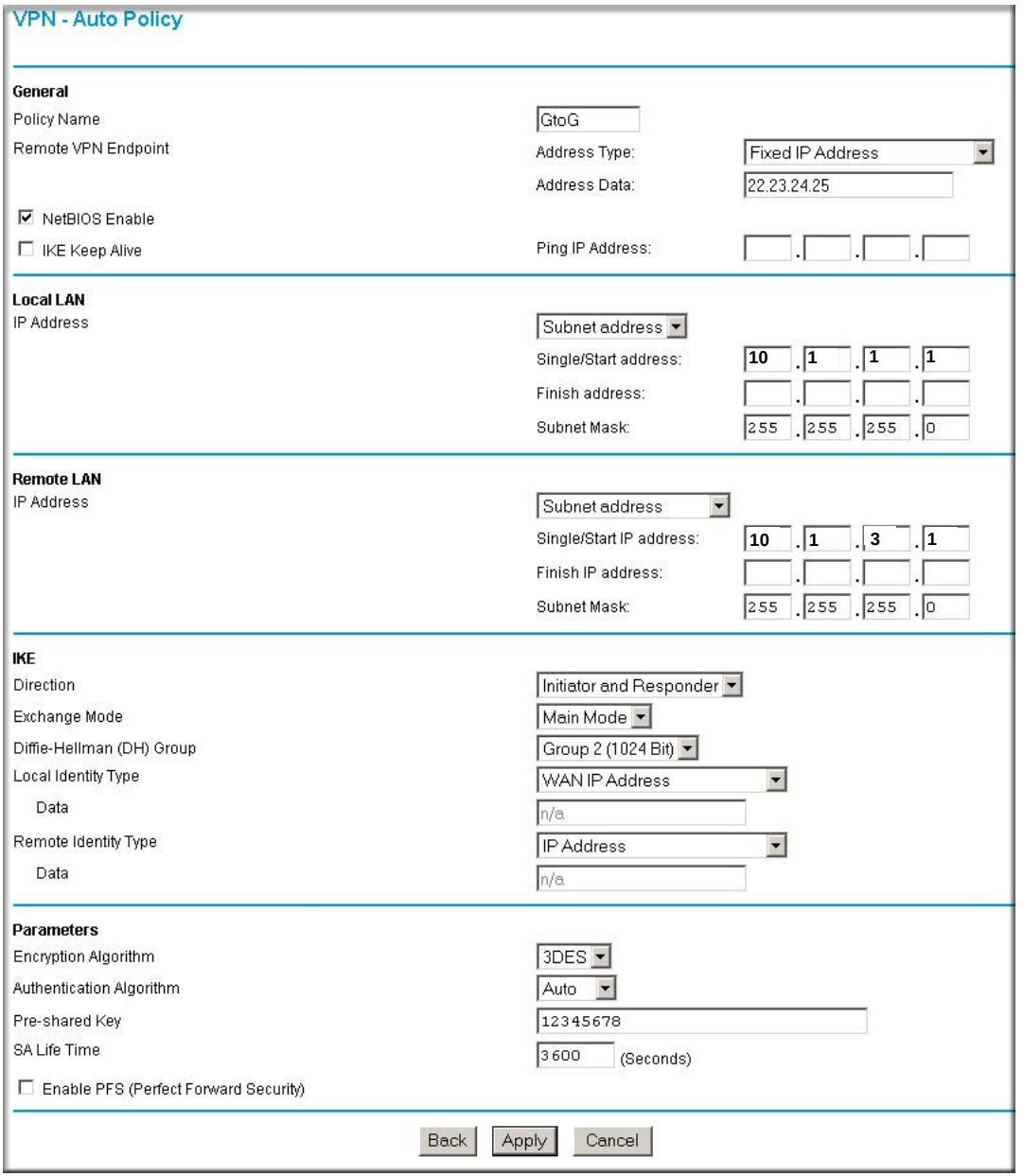



**Figure 8-40**

5. Click **Apply**. The Get VPN Policies web page is displayed.

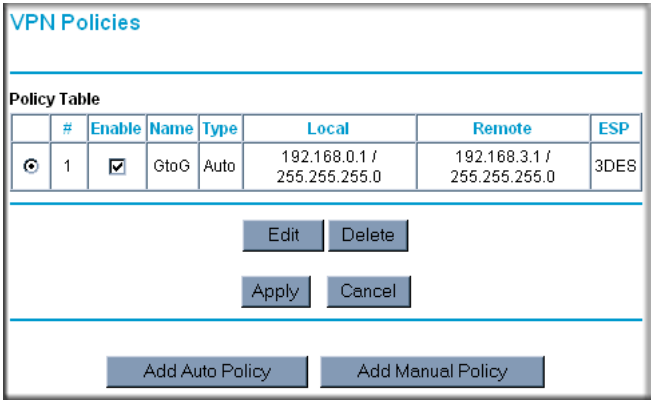



**Figure 8-41**

6. Repeat for the DG834GSP on LAN B and pay special attention to use the following network settings as appropriate.
   - General, Remote Address Data (e.g., **14.15.16.17**)
   - Remote LAN, Start IP Address
     - IP Address (e.g, **10.1.1.1**)
     - Subnet Mask (e.g., **255.255.255.0**)
     - Preshared Key (e.g., **12345678**)
7. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

**Note:** The VPN Status screen is only one of three ways to active a VPN tunnel. See "Activating a VPN Tunnel" on page 8-29 for information on the other ways.

**a.** Open the DG834GSP management interface and click on **VPN Status** to display the VPN Status/Log screen (Figure 8-42).

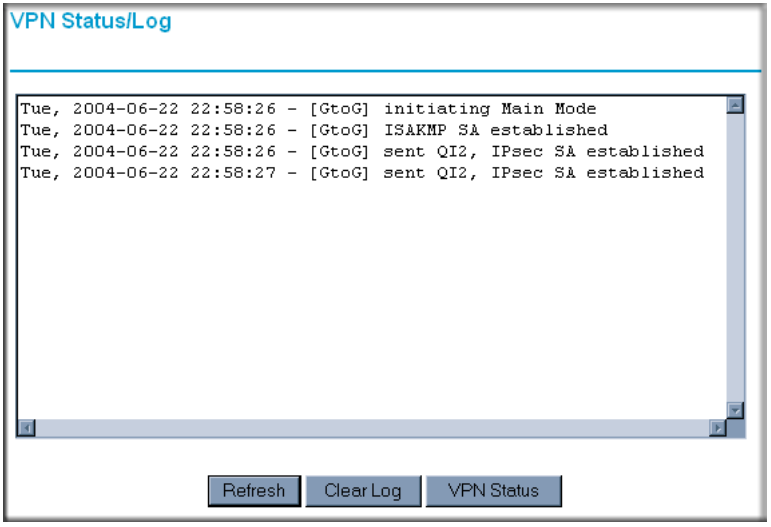

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

**Figure 8-42**

**b.** Click **VPN Status** (Figure 8-42) to display the Current VPN Tunnels (SAs) screen (Figure 8-43). Click on **Connect** for the VPN tunnel you want to activate.

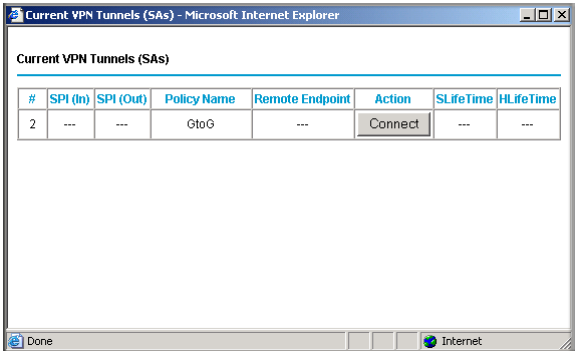

Current VPN Tunnels (SAs) - Microsoft Internet Explorer
Current VPN Tunnels (SAs)
# SPI (In) SPI (Out) Policy Name Remote Endpoint Action SLifeTime HLifeTime
2 --- --- GtoG --- Connect --- ---
Done
Internet

**Figure 8-43**

**c.** Review the VPN Status/Log screen (Figure 8-42) to verify that the tunnel is connected.

## Using Manual Policy to Configure VPN Tunnels

As an alternative to IKE, you may use Manual Keying, in which you must specify each phase of the connection. A "Manual" VPN policy requires all settings for the VPN tunnel to be manually input at each end (both VPN endpoints).

Click the **VPN Policies** link of the main menu, and then click the **Add Manual Policy** radio button to display the Manual Keys menu shown in Figure 8-44.

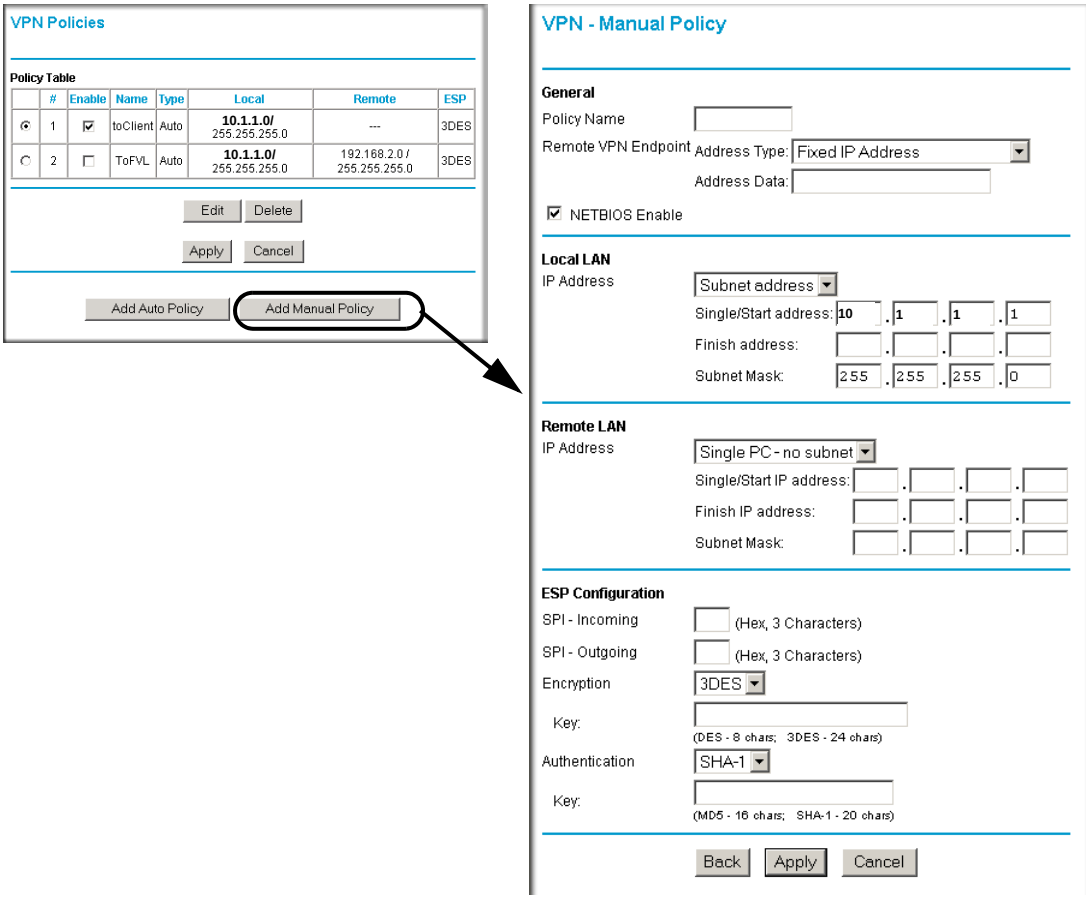



**Figure 8-44**

***General.*** The DG834GSP VPN tunnel network connection fields are defined as follows:

- **Policy Name**—enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**—select the desired option (IP address or Fully Qualified Domain Name) and enter the address of the remote VPN endpoint to which you wish to connect.

| | |
|---|---|
| | **Note:** The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint". |

***Local LAN.*** This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single address**—enter an IP address in the "Single/Start IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on your LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.
- **Any**—the remote VPN endpoint may be at any IP address.

The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.

***Remote LAN.*** This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single PC - no Subnet**—select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required.
- **Single address**—enter an IP address in the "Single/Start IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on the remote LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.

- **Any**—any outgoing traffic from the “Local IP” computers will trigger an attempted VPN connection to the remote VPN endpoint. Please be sure you want this option before selecting it.

The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.

***ESP Configuration.*** ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel.

**SPI**—enter the required security policy indexes (SPIs). Each policy must have unique SPIs. These settings must match the remote VPN endpoint. The "in" setting here must match the "out" setting on the remote VPN endpoint, and the "out" setting here must match the "in" setting on the remote VPN endpoint.

**Encryption**—select the desired Encryption Algorithm, and enter the key in the field provided. For 3DES, the keys should be 24 ASCII characters and for DES, the keys should be 8 ASCII characters.

- DES—the Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
- 3DES—(Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

**Authentication**—select the desired SHA-1 or MD5 Authentication Algorithm, and enter the key in the field provided. For MD5, the keys should be 16 ASCII characters. For SHA-1, the keys should be 20 ASCII characters.

- MD5—128 bits, faster but less secure.
- SHA-1 (default)—160 bits, slower but more secure.

# Chapter 9
# Troubleshooting

This chapter gives information about troubleshooting your 54 Mbps ADSL Modem Wireless Router Model DG834GSP. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?
- Have I connected the router correctly?

  Go to "Basic Functioning" on page 9-1.
- I can't access the router's configuration with my browser.

  Go to "Troubleshooting the Web Configuration Interface" on page 9-3.
- I've configured the router but I can't access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 9-4.
- I can't remember the router's configuration password.

  Go to "Restoring the Default Configuration and Password" on page 9-9.
- I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 9-9.

## Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on (see "The Router's Front Panel" on page 2-8 for an illustration and explanation of the LEDs).
2. Verify that the Test LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 10 seconds, verify that:
   a. The Test LED is not lit.
   b. The LAN port LEDs are lit for any local ports that are connected.

**c.** The WAN port LED is lit.

If a port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be amber.

If any of these conditions does not occur, refer to the appropriate following section.

## Power LED Not On

If the Power and other LEDs are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

## Test LED Never Turns On or Test LED Stays On

When the router is turned on, the Test LED turns on for about 10 seconds and then turns off. If the Test LED does not turn on, or if it stays on, there is a fault within the router.

If you experience problems with the Test LED:

- Cycle the power to see if the router recovers and the LED blinks for the correct amount of time.

If all LEDs including the Test LED are still on one minute after power up:

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This will set the router's IP address to 10.1.1.1. This procedure is explained in "Using the Reset button" on page 9-9.

If the error persists, you might have a hardware problem and should contact technical support.

## LAN or Internet Port LEDs Not On

If either the LAN LEDs or Internet LED do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
  - When connecting the router's WAN ADSL port, use the cable that was supplied with the DG834GSP.

## Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration interface from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 10.1.1.2 to 10.1.1.254. Refer to "Preparing a Computer for Network Access" in Appendix C to find your computer's IP address.

**Note:** If your computer's IP address is shown as 169.254.x.x:
Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 10.1.1.1. This procedure is explained in "Using the Reset button" on page 9-9.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the router does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

# Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should check the ADSL connection, then the WAN TCP/IP connection.

## ADSL link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.

Internet LED Green or Blinking Green

If your Internet LED is green or blinking green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

### Internet LED Blinking Amber

If your Internet LED is blinking amber, then your modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the Internet LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green Internet LED, there may be a problem with your wiring. If the telephone company has tested the ADSL signal at your Network Interface Device (NID), then you may have poor quality wiring in your house.

### Internet LED Off

If the Internet LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green Internet LED the problem may be one of the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It may be necessary to use a swapper if you ADSL signal is on pins 1 and 4 or the RJ-11 jack. The ADSL Modem Wireless Router uses pins 2 and 3.

## Obtaining a WAN IP Address

If your modem router is unable to access the internet, and your Internet LED is green or blinking green, you should determine whether the modem router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your modem router must request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

To check the WAN IP address from the browser interface:

1. Launch your browser and select an external site such as www.netgear.com.
2. Access the Main Menu of the modem router's configuration at http://10.1.1.1.
3. Under the Maintenance heading check that an IP address is shown for the WAN Port. If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a Multiplexing Method or Virtual Path Identifier/Virtual Channel Identifier parameter.
  Verify with your ISP the Multiplexing Method and parameter value, and update the router's ADSL Settings accordingly.
- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or PPP over ATM (PPPOA) login.

- If you have selected a login program, you may have incorrectly set the Service Name, User Name and Password. See "Troubleshooting PPPoE or PPPoA", below.
- Your ISP may check for your computer's host name.
  Assign the computer Host Name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:

  Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

  OR

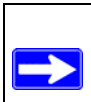
  Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu. Refer to the *ADSL Modem Wirelesss Router Setup Manual*.

## Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

1. Access the Main Menu of the router at http://10.1.1.1.
2. Under the Maintenance heading, select the **Router Status** link.
3. Click the **Connection Status** button.
4. If all of the steps indicate "OK" then your PPPoE or PPPoA connection is up and working.
5. If any of the steps indicates "Failed", you can attempt to reconnect by clicking **Connect**. The modem router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you may be using an incorrect Service Name, User Name or Password. There also may be a provisioning problem with your ISP.



Note: Unless you connect manually, the modem router will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

## Troubleshooting Internet Browsing

If your modem router can obtain an IP address but your computer is unable to load any Web pages from the Internet:

- Your computer may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the modem router's configuration, reboot your computer and verify the DNS address as described in "Preparing a Computer for Network Access" in Appendix C. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer may not have the modem router configured as its TCP/IP modem router.

  If your computer obtains its information from the modem router by DHCP, reboot the computer and verify the modem router address as described in "Preparing a Computer for Network Access" in Appendix C.

# Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer.

## Testing the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type Ping followed by the IP address of the router, as in this example:

   ```
   ping 10.1.1.1
   ```

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or Internet Port LEDs Not On" on page 9-2.
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - — Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

## Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where <*IP address*> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- — Check that your PC has the IP address of your router listed as the default modem router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default modem router as described in "Preparing a Computer for Network Access" in Appendix C.
- — Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- — Check that your cable or DSL modem is connected and functioning.

— If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC. Refer to your *ADSL Modem Wirelesss Router Setup Manual*.

## Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to 10.1.1.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the Web Configuration Manager (see "Backing Up, Restoring, or Erasing Your Settings" on page 6-1).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

### Using the Reset button

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).
2. Release the Default Reset button and wait for the router to reboot.

## Problems with Date and Time

The E-mail menu in the Content Filtering section displays the current date and time of day. The ADSL Modem Wireless Router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000
  Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour
  Cause: The router does not automatically sense Daylight Savings Time. In the E-mail menu, check or uncheck the box marked “Adjust for Daylight Savings Time”.

# Appendix A
# Technical Specifications

This appendix provides technical specifications for the 54 Mbps ADSL Modem Wireless Router Model DG834GSP.

| | |
|---|---|
| **Network Protocol and Standards Compatibility** | |
| Data and Routing Protocols: | TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPPoA, or PPTP, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM |
| **Power Adapter** | |
| North America: | 120V AC, 60 Hz, input |
| United Kingdom, Australia: | 240V AC, 50 Hz, input |
| Europe: | 230V AC, 50 Hz, input |
| Japan: | 100V AC, 50/60 Hz, input |
| All regions (output): | 12 V DC @ 1.0A output |
| **Physical Specifications** | |
| Dimensions: | 6.9" x 4.7" x 1.1"<br>175 mm x 119 mm x 28 mm |
| Weight: | 0.7 lbs.<br>0.3 kg |
| **Environmental Specifications** | |
| Operating temperature: | 0° to 40° C (32º to 104º F) |
| Operating humidity: | 90% maximum relative humidity, noncondensing |
| **Electromagnetic Emissions** | |
| Meets requirements of: | FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B |
| **Interface Specifications** | |
| LAN: | 10BASE-T or 100BASE-Tx, RJ-45 |
| WAN: | ADSL, ADSL2+, Dual RJ-11, pins 2 and 3,T1.413, G.DMT, G.Lite, ITU Annex A (for the DG834G) or ITU Annex B (for the DG834GB) |

# Appendix B
# NETGEAR VPN Configuration

## DG834GSP to FVL328

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DG834GSP to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

### Configuration Profile

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

**Table B-1. Profile Summary**

| | | |
|---|---|---|
| VPN Consortium Scenario: | | Scenario 1 |
| Type of VPN | | LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway) |
| Security Scheme: | | IKE with Preshared Secret/Key (not Certificate-based) |
| IP Addressing: | | |
| | NETGEAR-Gateway A | Static IP address |
| | NETGEAR-Gateway B | Static IP address |

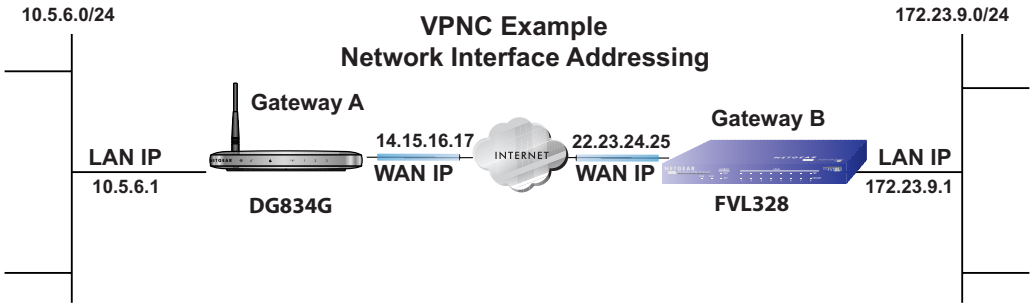



**Figure B-1**

**Note:** Product updates are available on the NETGEAR, Inc. web site at *http://kbserver.netgear.com/DG834GSP.asp*.

## Step-By-Step Configuration

1. Configure the DG834GSP as in the Gateway-to-Gateway procedures using the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 8-21), being certain to use appropriate network addresses for the environment.

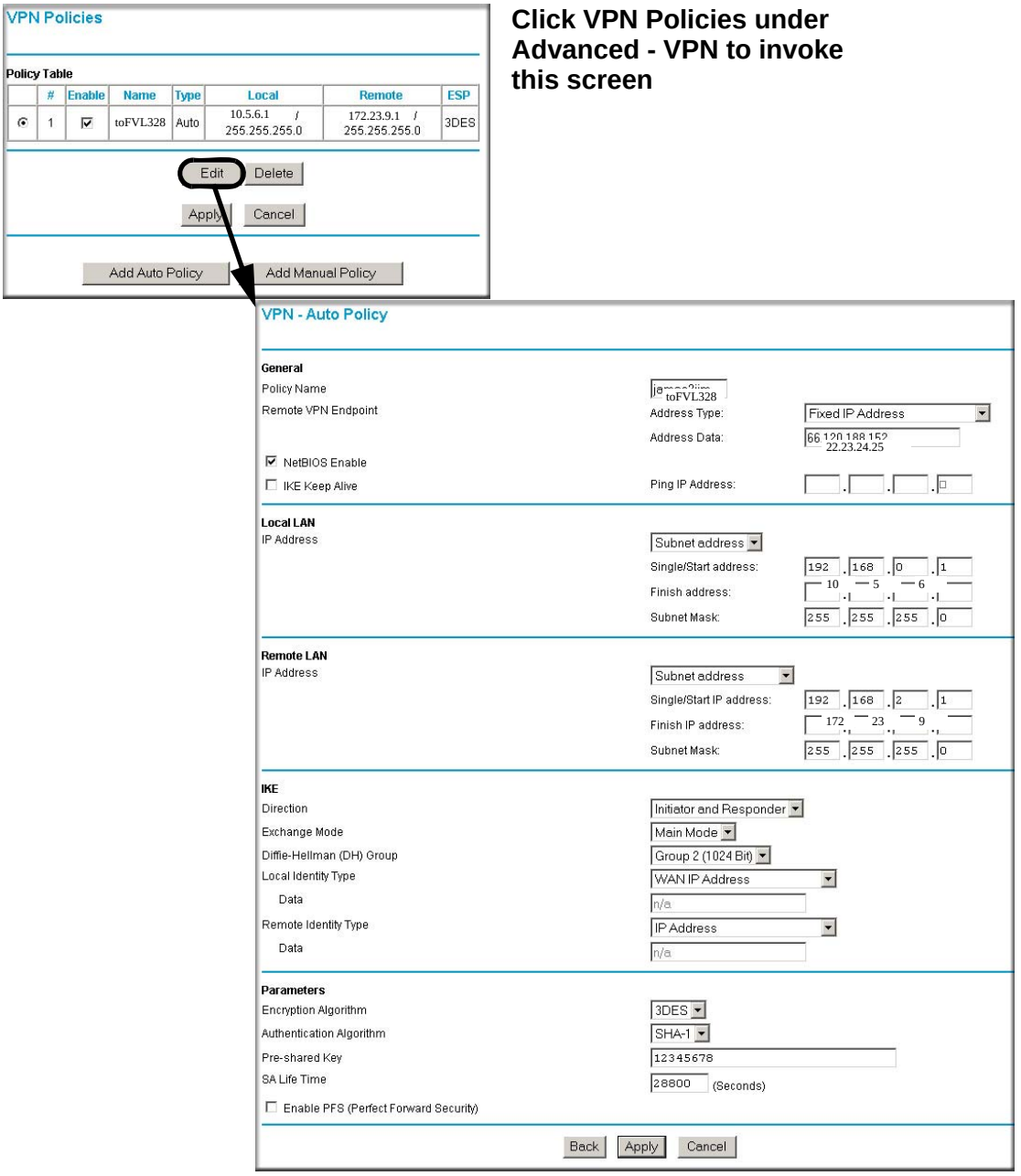
   The LAN Addresses used in this example are as follows:

| Unit | WAN IP | LAN IP | LAN Subnet Mask |
|---|---|---|---|
| DG834G | 14.15.16.17 | 10.5.6.1 | 255.255.255.0 |
| FVL328 | 22.13.24.25 | 172.23.9.1 | 255.255.255.0 |

   a. In Step 1, enter **toFVL328** for the Connection Name.

   b. In Step 2, enter **22.23.24.25** for the remote WAN's IP address.

   c. In Step 3, enter the following:
      - IP Address = **172.23.9.1**
      - Subnet Mask = **255.255.255.0**




**Click VPN Policies under Advanced - VPN to invoke this screen**

**Figure B-2**

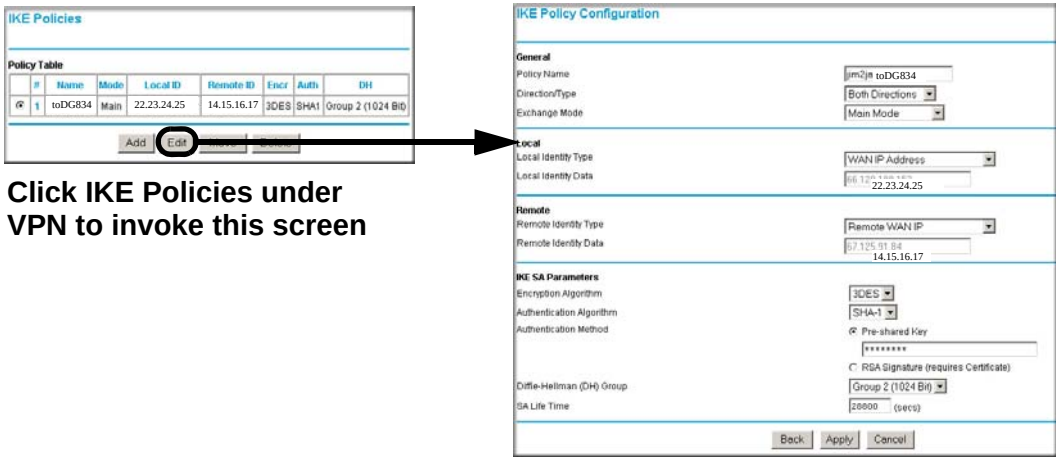
**2.** Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 8-21), being certain to use appropriate network addresses for the environment.

**a.** In Step 1, enter **toDG834** for the Connection Name

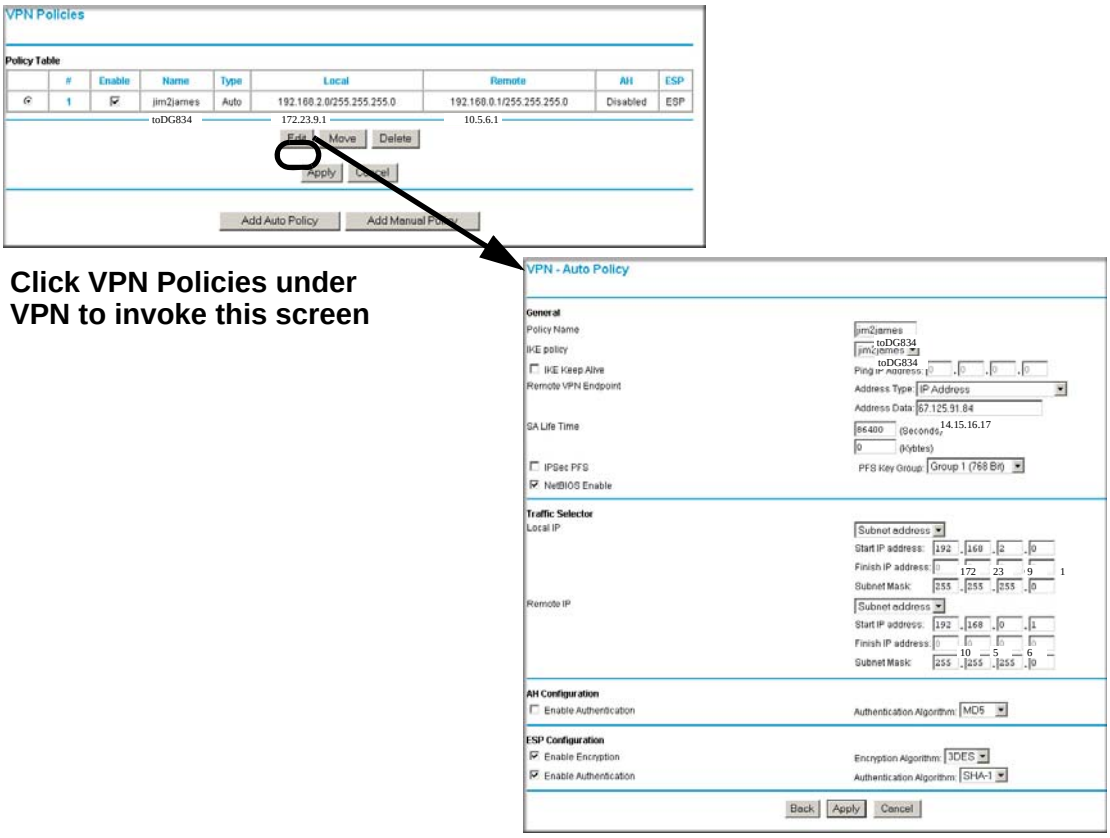
**b.** In Step 2, enter **14.15.16.17** for the remote WAN's IP address

**c.** In Step 3, enter the following:

- IP Address = **10.5.6.1**
- Subnet Mask = **255.255.255.0**




**Click IKE Policies under VPN to invoke this screen**




**Click VPN Policies under VPN to invoke this screen**

**Figure B-3**

3. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834GSP.
   a. Open the command prompt (Start -> Run -> cmd)
   b. ping 172.23.9.1

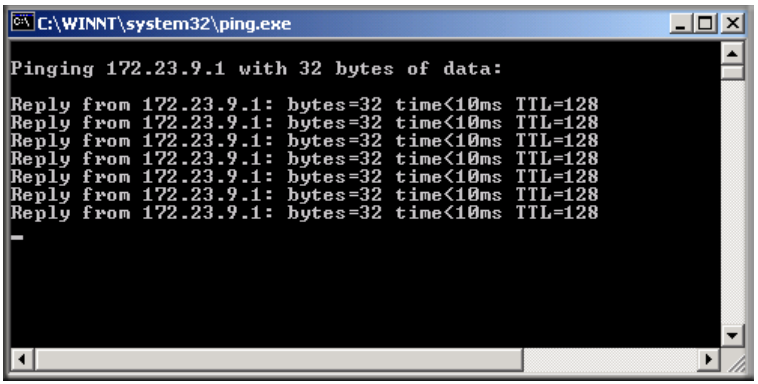

C:\WINNT\system32\ping.exe
Pinging 172.23.9.1 with 32 bytes of data:
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128

**Figure B-4**

**Note:** The pings may fail the first time. If this happens, try the pings a second time.

# DG834GSP with FQDN to FVL328

This appendix is a case study on how to configure a VPN tunnel from a NETGEAR DG834GSP to a FVL328 using a Fully Qualified Domain Name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

## Configuration Profile

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

**Table B-2. Profile Summary**

| | | |
|---|---|---|
| VPN Consortium Scenario: | | Scenario 1 |
| Type of VPN | | LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway) |
| Security Scheme: | | IKE with Preshared Secret/Key (not Certificate-based) |
| IP Addressing: | | |
| | NETGEAR-Gateway A | Fully Qualified Domain Name (FQDN) |
| | NETGEAR-Gateway B | FDQN |

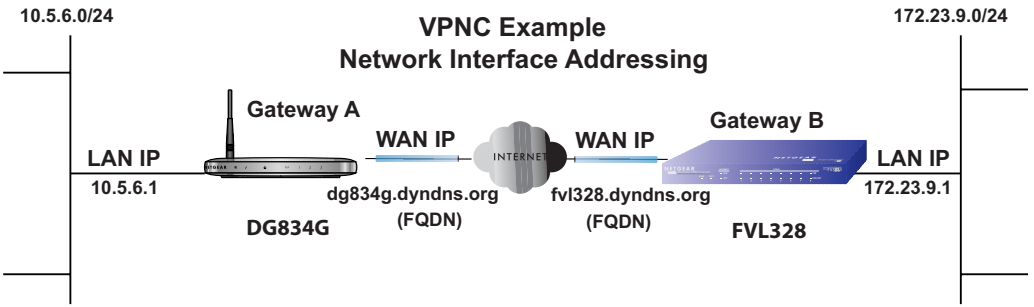



**Figure B-5**

**Note:** Product updates are available on the NETGEAR, Inc. web site at *http://kbserver.netgear.com/DG834GSP.asp*.

### The Use of a Fully Qualified Domain Name (FQDN)

Many ISPs (Internet Service Providers) provide connectivity to their customers using dynamic instead of static IP addressing. This means that a user's IP address does not remain constant over time which presents a challenge for gateways attempting to establish VPN connectivity.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host or domain name. It provides a central public database where information (such as email addresses, host names and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a 3rd party service in lieu of a permanent and unchanging IP address to establish bi-directional VPN connectivity.

To use DDNS, you must register with a DDNS service provider. Example DDNS Service Providers include:

- DynDNS: www.dyndns.org
- TZO.com: netgear.tzo.com
- ngDDNS: ngddns.iego.net

In this example, Gateway A is configured using an example FQDN provided by a DDNS Service provider. In this case we established the hostname **dg834g.dyndns.org** for gateway A using the DynDNS service. Gateway B will use the DDNS Service Provider when establishing a VPN tunnel.

In order to establish VPN connectivity Gateway A must be configured to use Dynamic DNS, and Gateway B must be configured to use a DNS hostname to find Gateway A provided by a DDNS Service Provider. Again, the following step-by-step procedures assume that you have already registered with a DDNS Service Provider and have the configuration information necessary to set up the gateways.

## Step-By-Step Configuration

**1.** Log in to the DG834GSP labeled Gateway A as in the illustration.

Out of the box, the DG834GSP is set for its default LAN address of http://10.1.1.1 with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

**2.** Click on the **Dynamic DNS** link on the left side of the Settings management GUI. This will take you to the Dynamic DNS Menu.

3. On the DG834GSP, configure the Dynamic DNS settings.

   a. Browse to the Dynamic DNS Setup Screen (see Figure B-6) in the Advanced menu.

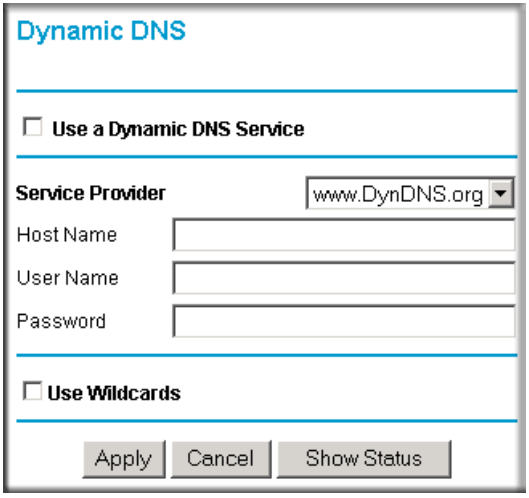



**Figure B-6**

   b. Configure this screen with appropriate account and hostname settings and then click **Apply**.

   - Check the box **Use a Dynamic DNS Service**.
   - Host Name = dg834g.dyndns.org
   - User Name = <user's account username>
   - Password = <user's account password>

   c. Click **Show Status**. The resulting screen should show Update OK: good (see Figure B-7).

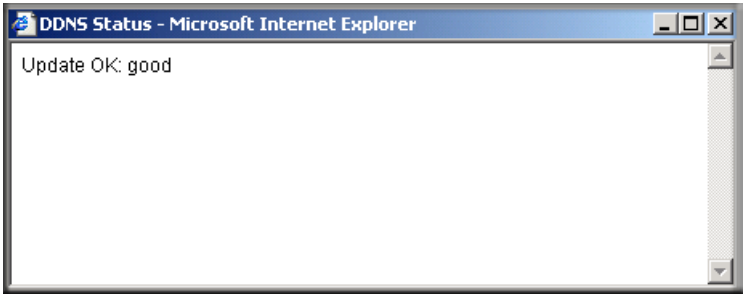



**Figure B-7**

4. On the FVL328, configure the Dynamic DNS settings. Assume a properly configured DynDNS account.

   a. Browse to the Dynamic DNS Setup Screen (see Figure B-8) in the Advanced menu.

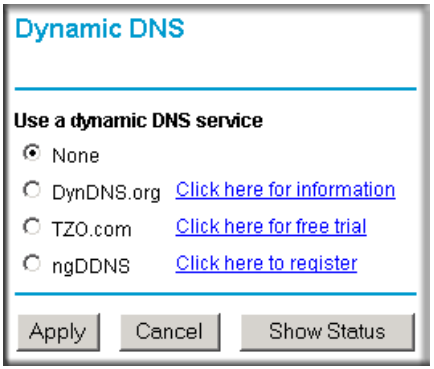



**Figure B-8**

   b. Select the **DynDNS.org** radio button (see Figure B-8), configure with appropriate account and hostname settings (see Figure B-9), and then click **Apply**.

   - Host and Domain Name = fvl328.dyndns.org
   - User Name = <user's account username>
   - Password = <user's account password>

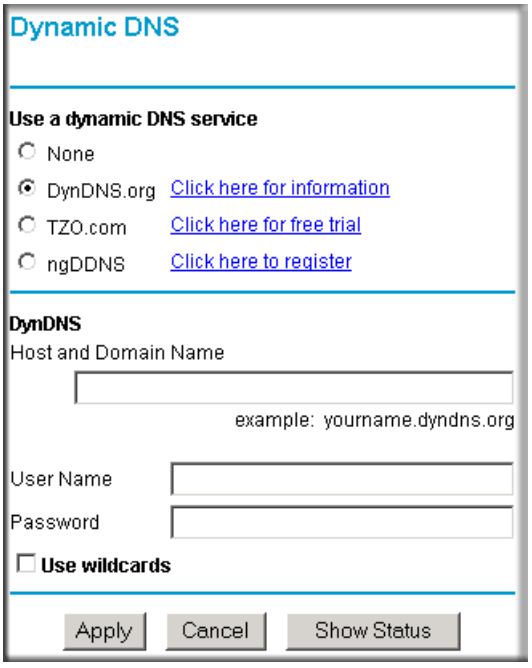



**Figure B-9**

**c.** Click **Show Status**. The resulting screen should show Update OK: good (see Figure B-10).

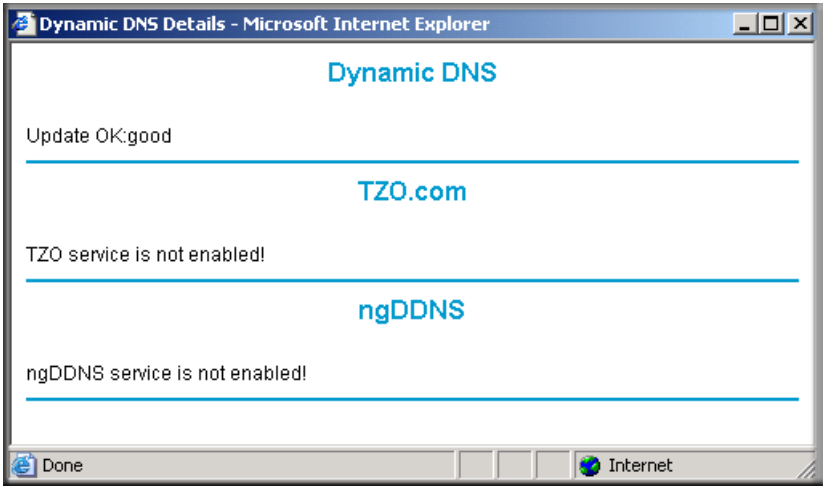



**Figure B-10**

5. Configure the DG834GSP as in the Gateway-to-Gateway procedures using the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 8-21), being certain to use appropriate network addresses for the environment.

   The LAN Addresses used in this example are as follows:

| Device | LAN IP Address | LAN Subnet Mask |
|---|---|---|
| DG834GSP | 10.5.6.1 | 255.255.255.0 |
| FVL328 | 172.23.6.1 | 255.255.255.0 |

   a. In Step 1, enter **toFVL328** for the Connection Name.

   b. In Step 2, enter **fvl328.dyndns.org** for the remote WAN's IP address.

   c. In Step 3, enter the following:
      - IP Address = **172.23.9.1**
      - Subnet Mask = **255.255.255.0**

6. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 8-21), being certain to use appropriate network addresses for the environment.

   a. In Step 1, enter **toDG834** for the Connection Name.

   b. In Step 2, enter **dg834g.dyndns.org** for the remote WAN's IP address.

   c. In Step 3, enter the following:
      - IP Address = **10.5.6.1**
      - Subnet Mask = **255.255.255.0**

7. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834GSP.

   a. Open the command prompt (Start -> Run -> cmd)

   b. ping 172.23.9.1

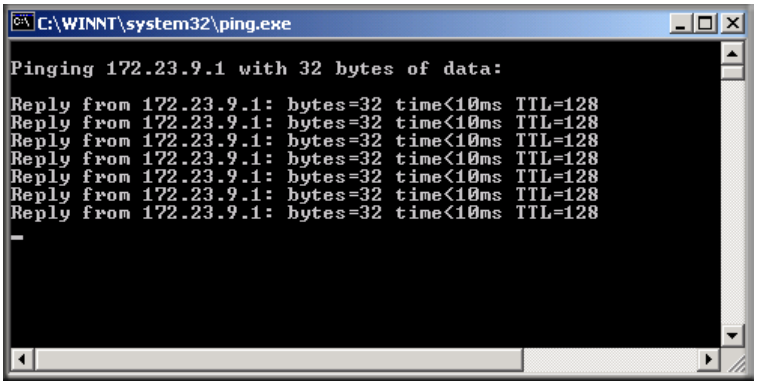

C:\WINNT\system32\ping.exe
Pinging 172.23.9.1 with 32 bytes of data:
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128

**Figure B-11**

**Note:** The pings may fail the first time. If this happens, try the pings a second time.

# Configuration Summary (Telecommuter Example)

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Assure that there are no firewall restrictions.

**Table B-3. Configuration summary (telecommuter example)**

| | | |
|---|---|---|
| VPN Consortium Scenario: | | Scenario 1 |
| Type of VPN: | | PC/client-to-gateway, with client behind NAT router |
| Security Scheme: | | IKE with Preshared Secret/Key (not Certificate-based) |
| IP Addressing: | | |
| | Gateway | Fully Qualified Domain Name (FQDN) |
| | Client | Dynamic |

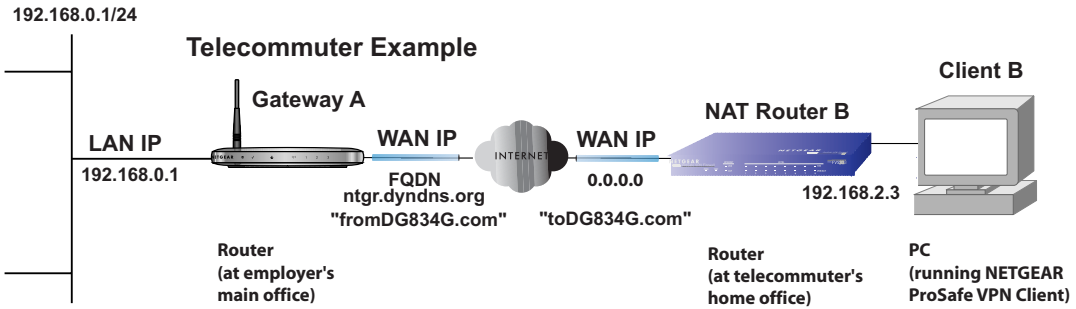



**Figure B-12**

# Setting Up the Client-to-Gateway VPN Configuration (Telecommuter Example)

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway involves the following two steps:

- Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office.

- Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office configures the NETGEAR ProSafe VPN Client endpoint.

## Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office

Follow this procedure to configure a client-to-gateway VPN tunnel by filling out the VPN Auto Policy screen.

1. Log in to the VPN router at its LAN address of http://10.1.1.1 with its default user name of **admin** and password of **password**. Click the **VPN Policies** link in the main menu to display the VPN Policies screen. Click **Add Auto Policy** to proceed and enter the information.

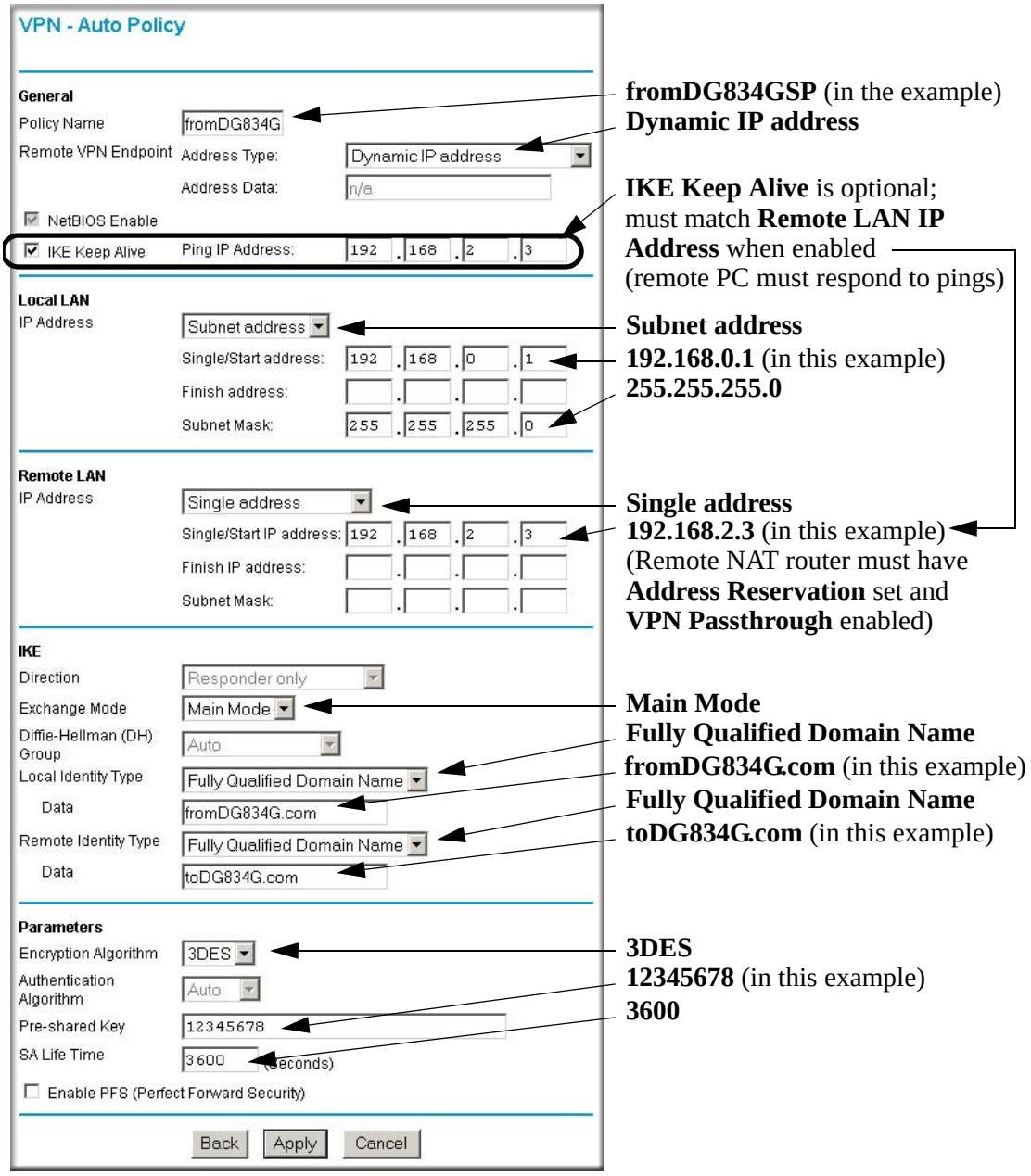

VPN - Auto Policy
General
Policy Name
fromDG834G
Remote VPN Endpoint
Address Type:
Dynamic IP address
Address Data:
n/a
NetBIOS Enable
IKE Keep Alive
Ping IP Address:
192 . 168 . 2 . 3
Local LAN
IP Address
Subnet address
Single/Start address:
192 . 168 . 0 . 1
Finish address:
Subnet Mask:
255 . 255 . 255 . 0
Remote LAN
IP Address
Single address
Single/Start IP address:
192 . 168 . 2 . 3
Finish IP address:
Subnet Mask:
IKE
Direction
Responder only
Exchange Mode
Main Mode
Diffie-Hellman (DH) Group
Auto
Local Identity Type
Fully Qualified Domain Name
Data
fromDG834G.com
Remote Identity Type
Fully Qualified Domain Name
Data
toDG834G.com
Parameters
Encryption Algorithm
3DES
Authentication Algorithm
Auto
Pre-shared Key
12345678
SA Life Time
3600
(seconds)
Enable PFS (Perfect Forward Security)
Back
Apply
Cancel
fromDG834GSP (in the example)
Dynamic IP address
IKE Keep Alive is optional; must match Remote LAN IP Address when enabled (remote PC must respond to pings)
Subnet address
192.168.0.1 (in this example)
255.255.255.0
Single address
192.168.2.3 (in this example)
(Remote NAT router must have Address Reservation set and VPN Passthrough enabled)
Main Mode
Fully Qualified Domain Name
fromDG834G.com (in this example)
Fully Qualified Domain Name
toDG834G.com (in this example)
3DES
12345678 (in this example)
3600

**Figure B-13**

2. Click **Apply** when done to get the **VPN Policies** screen.

**Figure B-14**

To view or modify the tunnel settings, select the radio button next to the tunnel entry and click **Edit**.

## Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office

This procedure describes how to configure the 54 Mbps ADSL Modem Wireless Router Model DG834GSP. We will assume the PC running the client has a dynamically assigned IP address.

The PC must have a VPN client program installed that supports IPSec (in this case study, the NETGEAR VPN ProSafe Client is used). Go to the NETGEAR website (*http://www.netgear.com*) and select **VPN01L_VPN05L** in the **Product Quick Find** drop-down menu for information on how to purchase the NETGEAR ProSafe VPN Client.

| | |
|---|---|
| | **Note:** Before installing the 54 Mbps ADSL Modem Wireless Router Model DG834GSP software, be sure to turn off any virus protection or firewall software you may be running on your PC. |

1. Install the NETGEA ProSafe VPN Client on the remote PC and reboot.
   a. You may need to insert your Windows CD to complete the installation.
   b. If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating "The **NETGEAR ProSafe VPN** Component requires at least one dial-up adapter be installed." You can disregard this message.
   c. Install the **IPSec** Component. You may have the option to install either the **VPN Adapter** or the **IPSec Component** or both. The **VPN Adapter** is not necessary.
   d. The system should show the **ProSafe** icon ( ) in the system tray after rebooting.
   e. Double-click the system tray icon to open the **Security Policy Editor**.
2. Add a new connection.
   a. Run the **NETGEAR ProSafe Security Policy Editor** program and create a **VPN Connection**.

**b.** From the **Edit** menu of the **Security Policy Editor**, click **Add**, then **Connection**. A **New Connection** listing appears in the list of policies. Rename the **New Connection** so that it matches the **Connection Name** you entered in the **VPN Settings** of the DG834GSP on Gateway A.

| | |
|---|---|
| | **Note:** In this example, the **Connection Name** used on the client side of the VPN tunnel is **to DG834GSP** and it does not have to match the **VPN_client Connection Name** used on the gateway side of the VPN tunnel (see Figure B-16) because Connection Names are arbitrary to how the VPN tunnel functions. |

| | |
|---|---|
| | **Tip:** Choose Connection Names that make sense to the people using and administrating the VPN. |

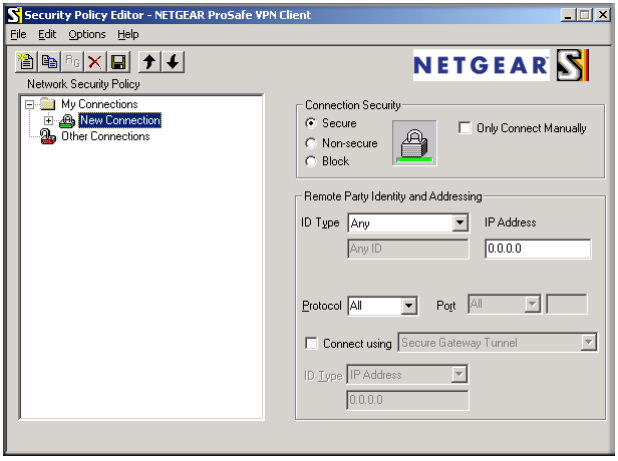



**Figure B-15**

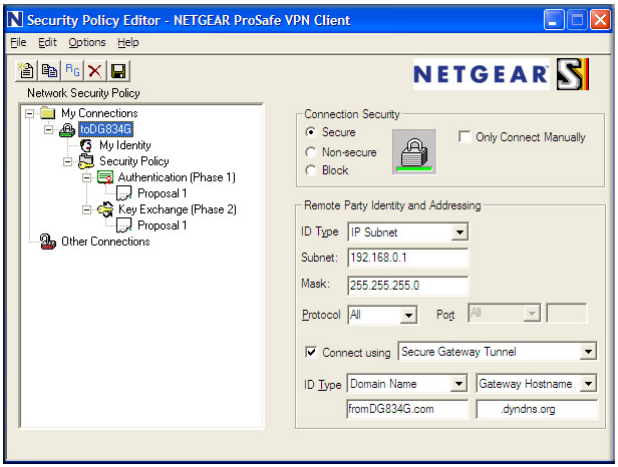



**Figure B-16**

**c.** Select **Secure** in the **Connection Security** check-box group.

**d.** Select **IP Subnet** in the **ID Type** menu.

**e.** In this example, type **10.1.1.1** in the Subnet field as the network address of the DG834GSP.

**f.** Enter **255.255.255.0** in the Mask field as the **LAN Subnet Mask** of the DG834GSP.

**g.** Select **All** in the **Protocol** menu to allow all traffic through the VPN tunnel.

**h.** Select the **Connect using Secure Gateway Tunnel** check box.

**i.** Select **Domain Name** in the **ID Type** menu below the check box and enter **fromDG834G.com** (in this example).

**j.** Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).

**k.** The resulting Connection Settings are shown in Figure B-16.

**3.** Configure the **Security Policy** in the 54 Mbps ADSL Modem Wireless Router Model DG834GSP software.

**a.** In the **Network Security Policy** list, expand the new connection by double clicking its name or clicking on the "+" symbol. **My Identity** and **Security Policy** subheadings appear below the connection name.

**b.** Click on the **Security Policy** subheading to show the **Security Policy** menu.

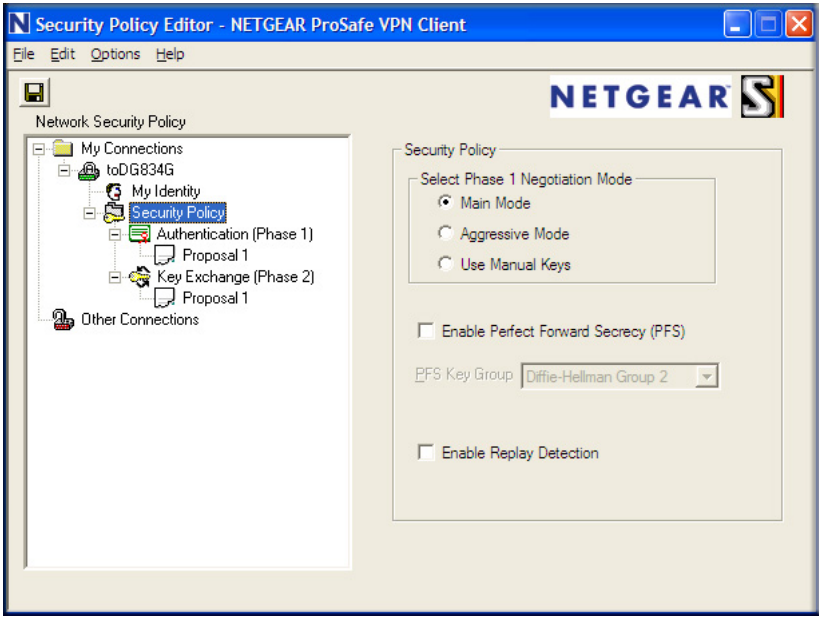



**Figure B-17**

**c.** Select the **Main Mode** in the **Select Phase 1 Negotiation Mode** check box.

**4.** Configure the **VPN Client Identity**.

In this step, you will provide information about the remote VPN client PC. You will need to provide the Pre-Shared Key that you configured in the DG834GSP and either a fixed IP address or a “fixed virtual” IP address of the VPN client PC.

**a.** In the **Network Security Policy** list on the left side of the **Security Policy Editor** window, click **My Identity**.

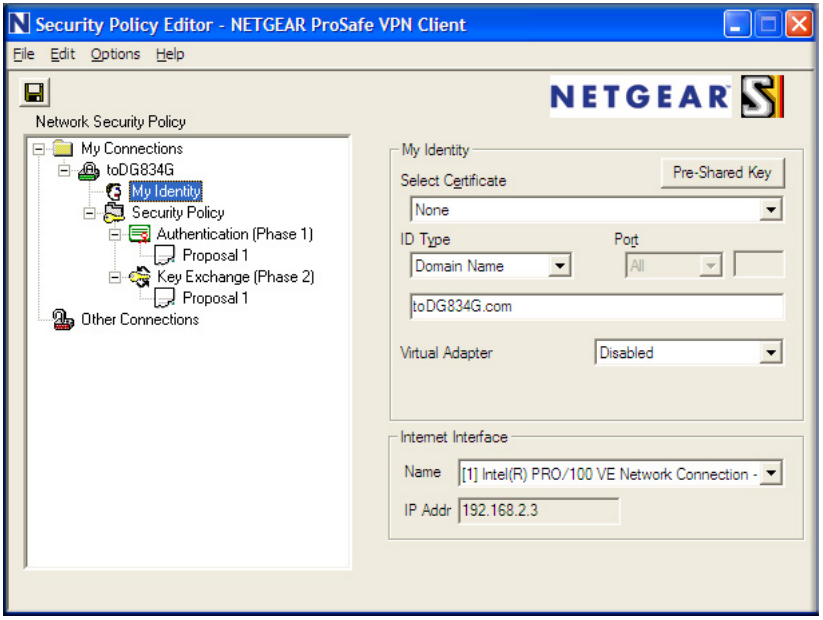



**Figure B-18**

**b.** Choose **None** in the **Select Certificate** menu.

**c.** Select **Domain Name** in the **ID Type** menu and enter **toDG834G.com** (in this example) in the box below it. Choose **Disabled** in the **Virtual Adapter** menu.

**d.** In the **Internet Interface** box, select **Intel PRO/100VE Network Connection** (in this example, your Ethernet adapter may be different) in the **Name** menu and enter **10.1.2.3** (in this example) in the **IP Addr** box.

**e.** Click the **Pre-Shared Key** button.

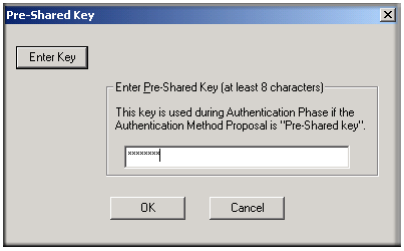

Pre-Shared Key
Enter Key
Enter Pre-Shared Key (at least 8 characters)
This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".
OK
Cancel

**Figure B-19**

**f.** In the **Pre-Shared Key** dialog box, click the **Enter Key** button. Enter the DG834GSP's **Pre-Shared Key** and click **OK**. In this example, **12345678** is entered. This field is case sensitive.

**5.** Configure the **VPN Client Authentication Proposal**.

In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the VPN router configuration.

**a.** In the **Network Security Policy** list on the left side of the **Security Policy Editor** window, expand the **Security Policy** heading by double clicking its name or clicking on the "+" symbol.

**b.** Expand the **Authentication** subheading by double clicking its name or clicking on the "+" symbol. Then select **Proposal 1** below **Authentication**.

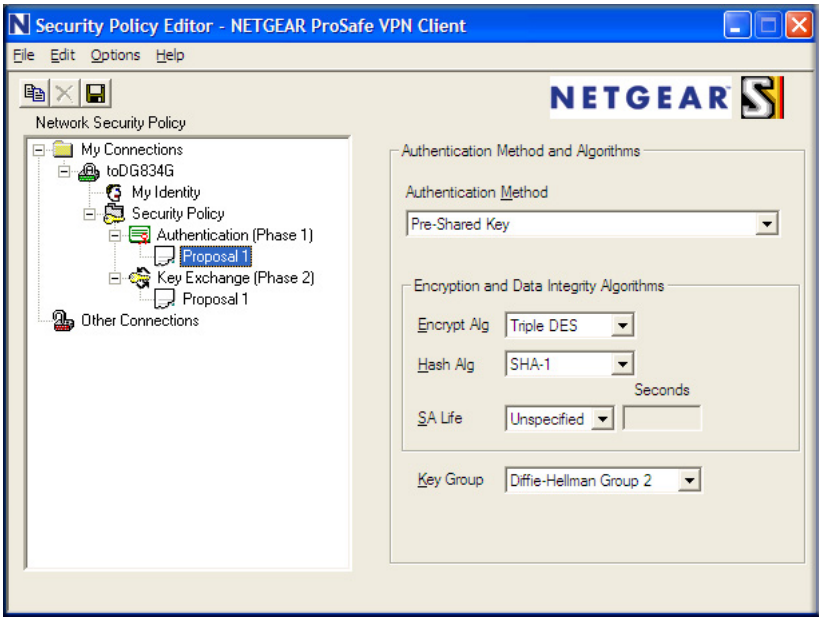



**Figure B-20**

**c.** In the **Authentication Method** menu, select **Pre-Shared key**.

**d.** In the **Encrypt Alg** menu, select the type of encryption. In this example, use **Triple DES**.

**e.** In the **Hash Alg** menu, select **SHA-1**.

**f.** In the **SA Life** menu, select **Unspecified**.

**g.** In the **Key Group** menu, select **Diffie-Hellman Group 2**.

**6.** Configure the **VPN Client Key Exchange Proposal**.

In this step, you will provide the type of encryption (**DES** or **3DES**) to be used for this connection. This selection must match your selection in the VPN router configuration.

**a.** Expand the **Key Exchange** subheading by double clicking its name or clicking on the "+" symbol. Then select **Proposal 1** below **Key Exchange**.

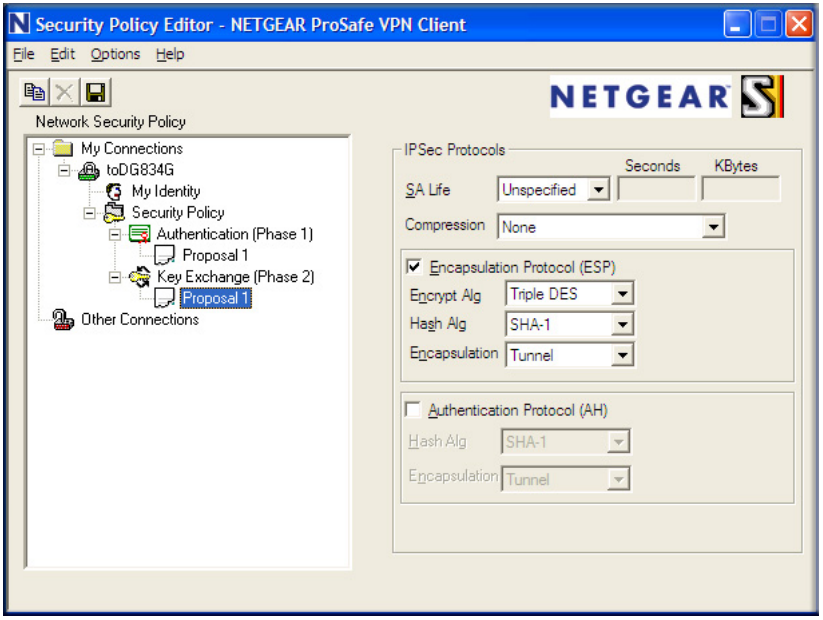



**Figure B-21**

**b.** In the **SA Life** menu, select **Unspecified**.

**c.** In the **Compression** menu, select **None**.

**d.** Check the **Encapsulation Protocol (ESP)** checkbox.

**e.** In the **Encrypt Alg** menu, select the type of encryption. In this example, use **Triple DES**.

**f.** In the **Hash Alg** menu, select **SHA-1**.

**g.** In the **Encapsulation** menu, select **Tunnel**.

**h.** Leave the **Authentication Protocol (AH)** checkbox unchecked.

**7.** Save the VPN Client settings.

From the **File** menu at the top of the **Security Policy Editor** window, select **Save**.

After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router's LAN.

**8.** Check the **VPN Connection**.

To check the **VPN Connection**, you can initiate a request from the remote PC to the VPN router's network by using the **Connect** option in the ADSL Modem Wireless Router menu bar (see Figure B-22). Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

**a.** Right-click the system tray icon to open the popup menu.

**b.** Select **Connect** to open the **My Connections** list.

**c.** Choose **toDG834G**.

The 54 Mbps ADSL Modem Wireless Router Model DG834GSP will report the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.

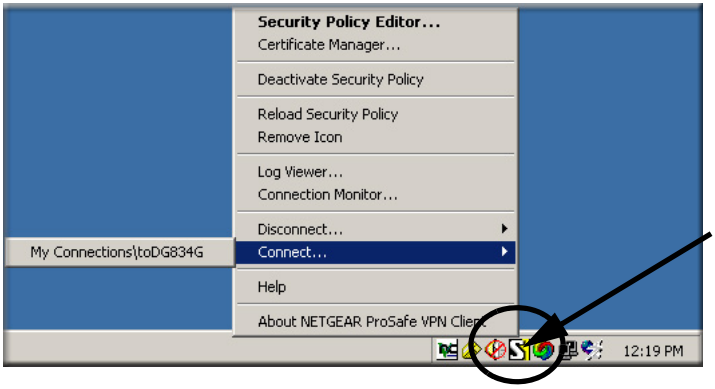



**Figure B-22**

To perform a ping test using our example, start from the remote PC:

**a.** Establish an Internet connection from the PC.

**b.** On the **Windows** taskbar, click the **Start** button, and then click **Run**.

**c.** Type **ping -t 10.1.1.1**, and then click **OK**.

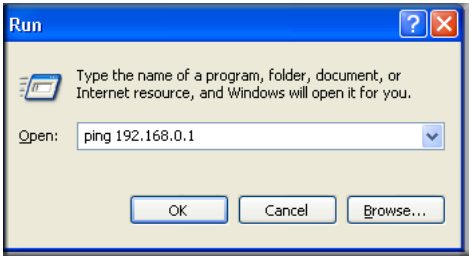



**Figure B-23**

This will cause a continuous ping to be sent to the VPN router. After between several seconds and two minutes, the ping response should change from **timed out** to **reply**.

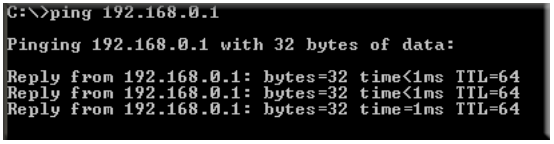

C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

**Figure B-24**

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the VPN router. After a short wait, you should see the login screen of the VPN router (unless another PC already has the VPN router management interface open).

**Note:** You can use the VPN router diagnostic utilities to test the VPN connection from the VPN router to the client PC. Run ping tests from the **Diagnostics** link of the VPN router main menu.

# Monitoring the VPN Tunnel (Telecommuter Example)

## Viewing the PC Client's Connection Monitor and Log Viewer

To view information on the progress and status of the VPN client connection, open the 54 Mbps ADSL Modem Wireless Router Model DG834GSP **Log Viewer**.

1. To launch this function, click on the Windows **Start** button, then select **Programs**, then **54 Mbps ADSL Modem Wireless Router Model DG834GSP**, then **Log Viewer**.

> **Note:** Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

2. The **Connection Monitor** screen is shown below:

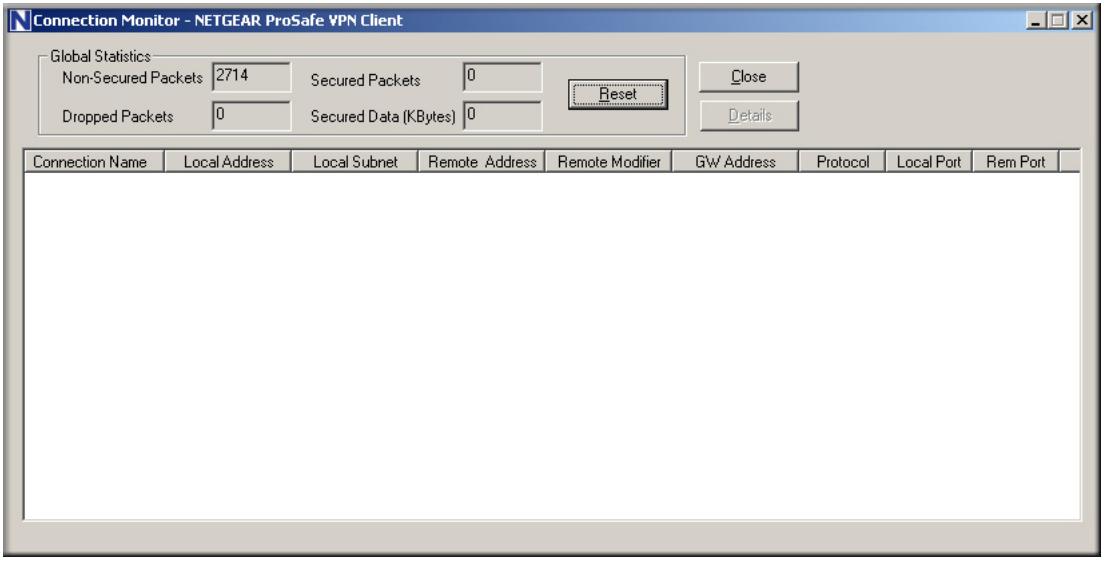



**Figure B-25**

While the connection is being established, the **Connection Name** field in this menu will show **SA** before the name of the connection. When the connection is successful, the **SA** will change to the yellow key symbol.

**Note:** While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you will need to close the VPN connection in order to have normal Internet access.

## Viewing the VPN Router's VPN Status and Log Information

To view information on the status of the VPN client connection, open the VPN router's VPN Status screen by following the steps below:

1. To view this screen, click the **Router Status** link of the VPN router's main menu, then click the **VPN Status** button. The **VPN Status/Log** screen for a connection is shown below:

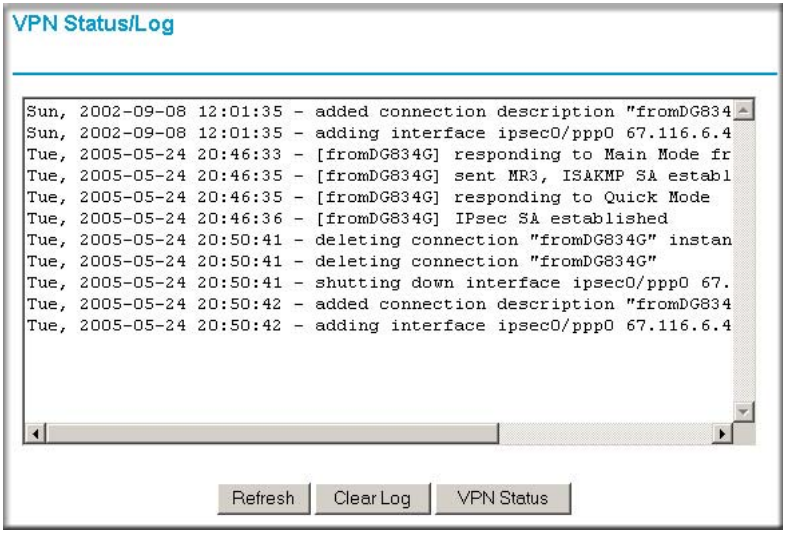

VPN Status/Log
Sun, 2002-09-08 12:01:35 - added connection description "fromDG834
Sun, 2002-09-08 12:01:35 - adding interface ipsec0/ppp0 67.116.6.4
Tue, 2005-05-24 20:46:33 - [fromDG834G] responding to Main Mode fr
Tue, 2005-05-24 20:46:35 - [fromDG834G] sent MR3, ISAKMP SA establ
Tue, 2005-05-24 20:46:35 - [fromDG834G] responding to Quick Mode
Tue, 2005-05-24 20:46:36 - [fromDG834G] IPsec SA established
Tue, 2005-05-24 20:50:41 - deleting connection "fromDG834G" instan
Tue, 2005-05-24 20:50:41 - deleting connection "fromDG834G"
Tue, 2005-05-24 20:50:41 - shutting down interface ipsec0/ppp0 67.
Tue, 2005-05-24 20:50:42 - added connection description "fromDG834
Tue, 2005-05-24 20:50:42 - adding interface ipsec0/ppp0 67.116.6.4
Refresh
Clear Log
VPN Status

**Figure B-26**

2. To view the VPN tunnels status, click the **VPN Status** link on the right side of the main menu.

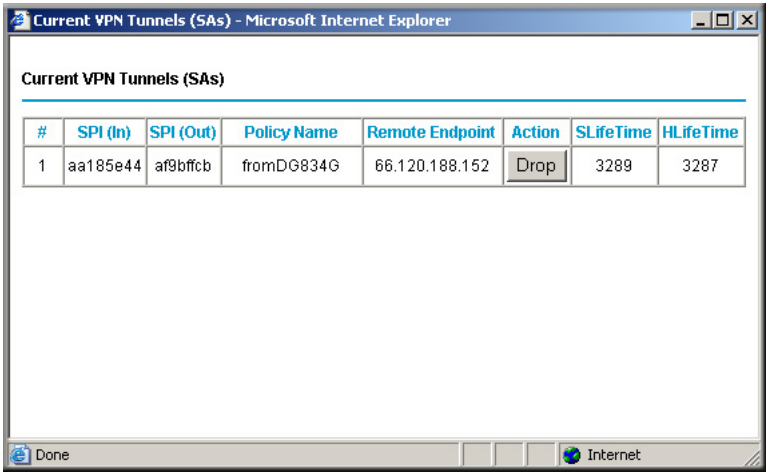

Current VPN Tunnels (SAs) - Microsoft Internet Explorer
Current VPN Tunnels (SAs)
# SPI (In) SPI (Out) Policy Name Remote Endpoint Action SLifeTime HLifeTime
1 aa185e44 af9bffcb fromDG834G 66.120.188.152 Drop 3289 3287
Done
Internet

**Figure B-27**

# Appendix C
# Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

| Document | Link |
|---|---|
| Internet Networking and TCP/IP Addressing | http://documentation.netgear.com/reference/enu/tcpip/index.htm |
| Wireless Communications | http://documentation.netgear.com/reference/enu/wireless/index.htm |
| Preparing a Computer for Network Access | http://documentation.netgear.com/reference/enu/wsdhcp/index.htm |
| Virtual Private Networking (VPN) | http://documentation.netgear.com/reference/enu/vpn/index.htm |
| Glossary | http://documentation.netgear.com/reference/enu/glossary/index.htm |